



Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



# ***Fair Information Practice Principles (FIPPS)***

Shannon Dahn  
Privacy Lead, Transformation  
Office of Privacy, USCIS  
[shannon.r.dahn@uscis.dhs.gov](mailto:shannon.r.dahn@uscis.dhs.gov)

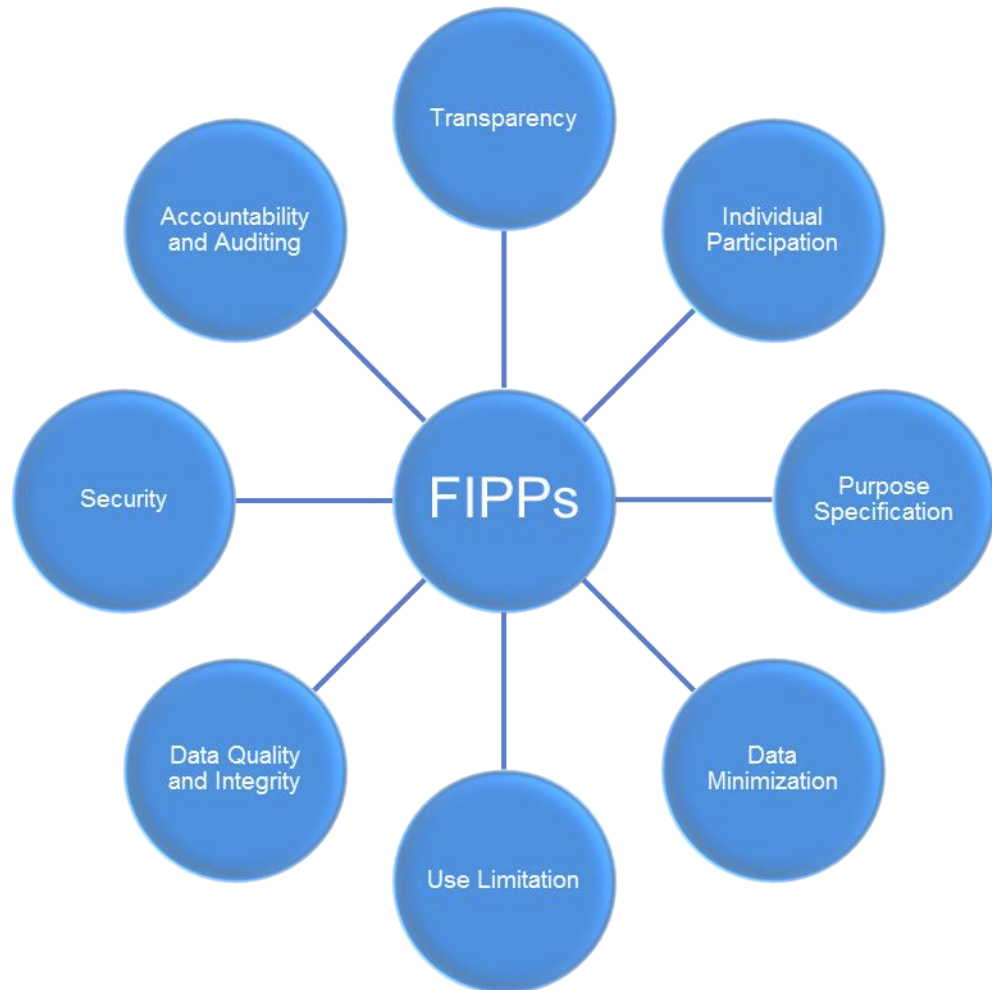
# Fair Information Practice Principles

- Department of Health, Education and Welfare's 1973 report entitled *Records, Computers and the Rights of Citizens* (1973), known as the *HEW Report*
  - The *HEW Report* led to the passage of the U.S. Privacy Act of 1974
- FIPPs based frameworks adopted worldwide:
  - U.S. Privacy Act
  - OECD Privacy Principles
  - Canadian PIPEDA
  - APEC Privacy Framework



# Fair Information Practice Principles

- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability and Auditing



# Fair Information Practice Principles at DHS

- FIPPs form the basis of the Department's privacy compliance policies and procedures governing the use of personally identifiable information (PII)

**DHS Policy** Reference: *DHS Privacy Policy Guidance Memorandum 2008-01 (December 29, 2008)*



**Homeland  
Security**

| Privacy Office



# DHS Definition of PII

- Personally Identifiable Information
  - DHS Definition: Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department



# FIPPS: Wait, Why Do I Care?

- Provides the *how* to conduct privacy analysis and improve privacy controls
- Framework upon which privacy compliance documents
- Use when encountering new technologies and creating new processes



**Homeland  
Security**

| Privacy Office

# Role of the Privacy Analyst

- Privacy analyst's checklist:
  1. Is there **PII**? Is it SPPII?
  2. From what **type of individual** is the PII collected?
  3. Analyze the program's collection and use of PII based on the **FIPPs**



# Transparency

- Provide **notice to the individual** regarding its collection, use, dissemination, and maintenance of personally identifiable information.
- Examples of transparency:
  - A Privacy Act Statement on a form at time of collection
  - Privacy Impact Assessments published on website
  - Signs that say, “This area monitored by Closed Circuit TV.”



# Individual Participation

- Collect information directly from the individual
- Seek individual consent for the collection, use, dissemination, and maintenance of PII.
- Examples of individual participation:
  - Almost all collections of information by DHS are voluntary, with the exception of law enforcement and intelligence operations



# Purpose Specification

- Specifically articulate the purpose(s) for which the PII is intended to be used.
- Articulate specific authority for collecting and using data in that way.
- Example:
  - Social Security numbers are authorized for certain purposes, and that use is appropriate if identified, articulate, and specified.



# Data Minimization

- DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- Example:
  - Programs should collect only the **minimum amount of information necessary to accomplish their mission**
  - Retain information minimum amount of time necessary to accomplish mission





# Use Limitation

- DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
- Example:
  - Social Security number is authorized for employment authorization processes, not to be used as a DHS account number just because we have it.



# Data Quality and Integrity

- DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- Example:
  - Privacy risk of DHS making a benefit determination for an individual based on incorrect data.



# Security

- DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- Examples:
  - Technical controls on data
  - Role-based access to data



# Accountability and Auditing

- DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.
- Examples:
  - Building in privacy compliance reviews
  - Strong audit capabilities in the data





# Homeland Security



Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



# ***Privacy Threshold Analysis (PTA)***

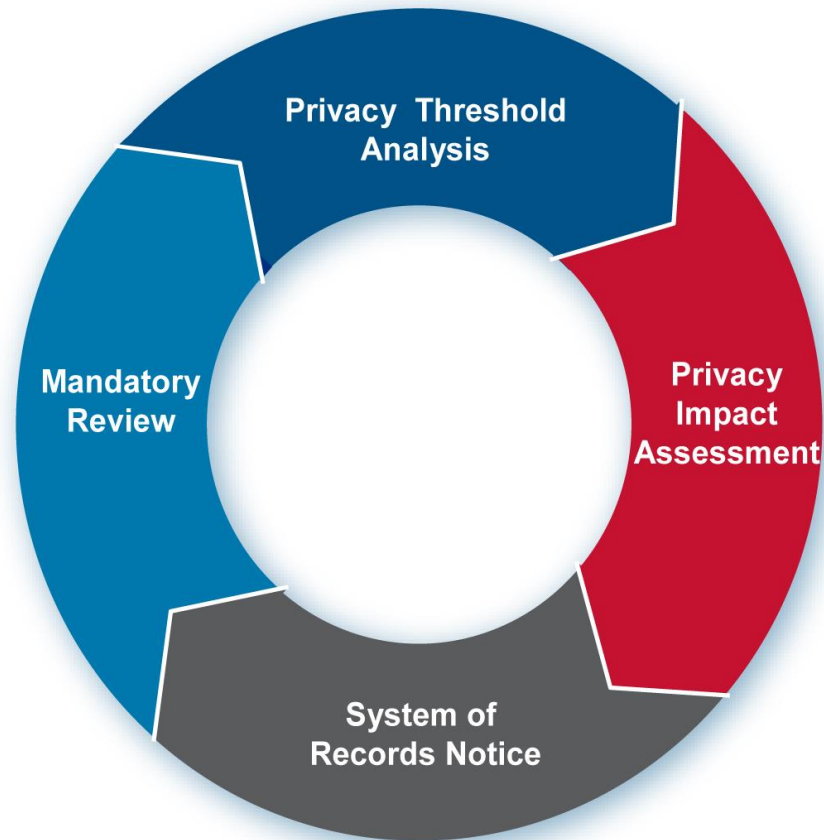
Lindsay Lennon

Privacy Analyst

DHS Privacy Office

[lindsay.lennon@hq.dhs.gov](mailto:lindsay.lennon@hq.dhs.gov)

# Privacy Compliance Process



**Homeland  
Security**

| Privacy Office



# Why complete a PTA?

- To demonstrate that privacy has been considered during the review of any new or updated program, project, process, or technology.
- To provide a record of a privacy-sensitive system and its privacy requirements in our tracking database.
- To demonstrate compliance with privacy laws and regulations as required by the Office of Inspector General (OIG) and Government Accountability Office (GAO) during reviews.



# When to complete a new PTA

- For a new project
- For IT security
- When a project makes changes
  - Collect new PII
  - Use the PII for a different purpose
  - Reduction of PII
- Every three years



# Who is responsible for PTAs at DHS?

- Component ISSOs\*/Program Managers
- Component Privacy Officers/Privacy Points of Contact (PPOCs)
- DHS Privacy Office

\* Information System Security Officer



**Homeland  
Security**

| Privacy Office

# PTA Questions

1. Reason for submitting the PTA (i.e., new, update, renewal) and Description and purpose of the project, program, or system
2. Technologies used
3. From whom does the Project or Program collect, maintain, use, or disseminate information?



# PTA Questions Continued

4. What specific information about individuals is collected, generated, or retained?
  - a. Does the project, program, or system retrieve information by personal identifier?
  - b. Does the project, program, or system use SSNs?
  - c. If yes, what is the specific legal authority?
  - d. If yes, describe how the project, program, or system will use SSN.
  - e. If the project, program, or system is an IT system, does it relate only to infrastructure?
  - f. What, if any, header or payload data is stored in the communications traffic log?



# PTA Questions Continued

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems?
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?
  - a. Is this external sharing pursuant to new or existing information sharing access agreement ?



# PTA Questions Continued

7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?
8. Does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?
9. Is there a FIPS 199 determination?





# Adjudication

## Component Privacy Officer Review

- Component privacy officers are the initial PTA point of contact with the programs
- Based on their initial analysis of privacy risks, they submit recommendations to DHS PRIV:
  - Existing PIA coverage (list PIA)
  - Existing SORN coverage (list SORN)
  - New PIA or SORN needed
- DHS PRIV analysts review recommendation and either concur or request additional explanation/analysis



# Adjudication

## DHS Privacy Office Adjudication

- Is the project, program, or system privacy sensitive?
  - If no, then the PTA adjudication is complete
- Category of System
  - IT System
  - National Security System
  - Legacy System
  - HR System
  - Rule
  - Form/Information Collection
  - Other



# Adjudication

## Determination

- PTA sufficient at this time.
- Privacy compliance documentation determination in progress.
- New information sharing arrangement is required.
- DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies.
- Privacy Act Statement required.
- Privacy Impact Assessment (PIA) required.
- System of Records Notice (SORN) required.
- Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.
- A Records Schedule may be required. Contact your component Records Officer



# Why should your organization use the PTA?

- Assists in determining privacy-sensitive systems, processes, and programs
- Easy to use format
- Provides better understanding to your Privacy Office
- Memorializes privacy documentation determinations





# Homeland Security



Homeland  
Security

Privacy Office

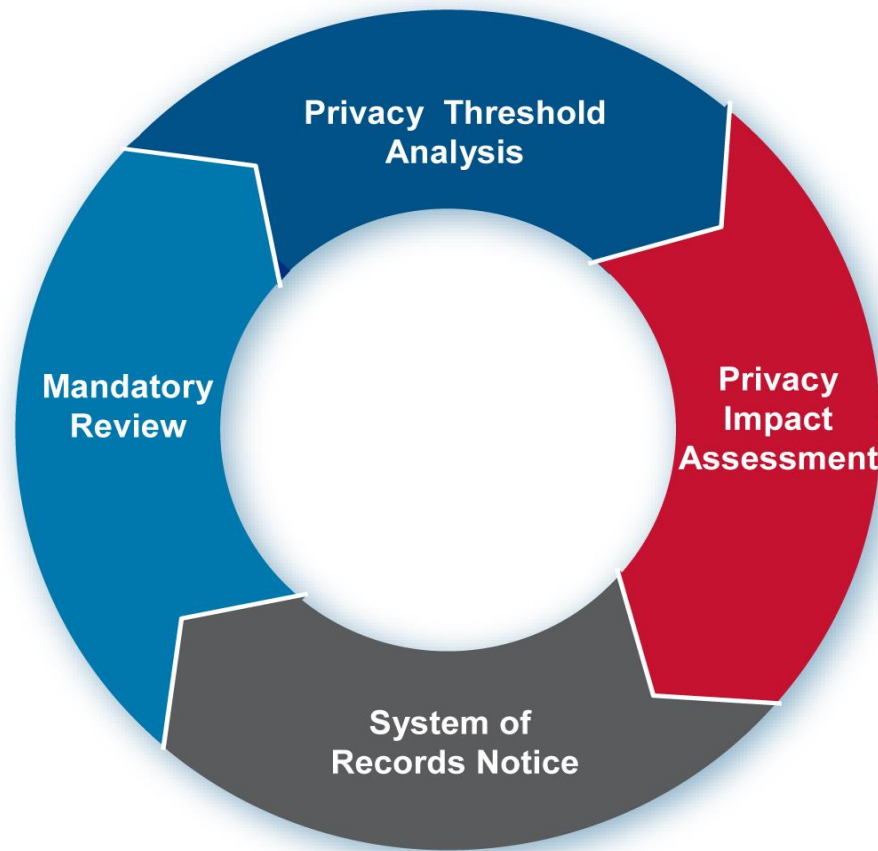
Protecting privacy while promoting transparency



# ***Privacy Impact Assessments (PIA)***

Jameson Morgan  
Privacy Analyst  
DHS Privacy Office

# Privacy Compliance Process





# What is a Privacy Impact Assessment (PIA)?

- A decision tool used by DHS to identify and mitigate privacy risks that notifies the public:
  - What PII DHS is collecting
  - Why the PII is being collected
  - How the PII will be used, shared, accessed, and stored.
- A successful PIA should accomplish three goals:
  - Ensure conformance with applicable legal, regulatory, and policy requirements for privacy;
  - Determine the **risks and effects**; and
  - Evaluate **protections** and alternative processes to **mitigate potential privacy risks**.



# Privacy Impact Assessments

## *Pursuant to Privacy Policy Guidance Memorandum 2008-02*

- PIAs are required for
  - IT systems that use, maintain, or disseminate PII, or when initiating a new collection of PII from ten or more individuals in the public ([E-Government Act, Section 208](#))
- DHS – Supplemental Requirements
  - Certain programs and activities of the Department, as required by Congress (Section 222(a)(4) HSA)
  - Rulemakings proposed by DHS that implicate privacy (Section 222(a)(4))
  - National security systems (conducted, not nec. published)
  - Multi-component HR systems (when PII pertains to employees/contractors of two or more DHS components)



# Conduct a PIA when...

- Developing or procuring **any new technologies or systems** that handle or collect PII, or that may have privacy implications.
- Developing **system revisions** that contribute to new privacy risks.
- Issuing a **new or updated rulemaking** that entails the collection of **PII**.
  - Even if a component has specific legal authority to collect certain information or build a certain program or system, a PIA is required.



# When is a PIA NOT required?

- When the PTA is adjudicated as not privacy sensitive
- No PII collected as determined in an adjudicated PTA from the Privacy Office
- HR systems that only collect on one component
- Already have an existing PIA and changes don't require an update per the PTA
- Note: DHS PRIV provides guidance on whether or not a PIA is required for any DHS program, system, project, or other information collection.



# Specialized PIAs

- DHS-Wide PIAs
  - Contact Lists
  - SharePoint
  - CCTV
  - FIPPS
  - DHS Web Portals
  - Social Media
  - ISE SAR
- Complete a specialized PTA. If the program adheres to the rules, it will be covered by the appropriate DHS-Wide PIA and added to the Appendix.
- PIA Update Template



# Process and Document

- **Iterative process** with program, legal counsel, IT and Privacy Office collaborating
- **Start at the beginning** of a new program and build in privacy



# DHS PIA Template

- Guidance is embedded within the template
- Designed to meet requirements set by law, guidance, and policy
- First page gives overall instructions
- Questions cannot be deleted/edited
- Formatting should not change **unless DHS PRIV makes the edits**



# PIA: Abstract

The abstract is the single paragraph that will be used to describe the program and the PIA. It will be published on the DHS web site and Federal Register. It should be a minimum of three sentences and a maximum of four, and conform to the following format:

- First sentence:
  - name of the component and the system
- Second sentence:
  - Brief description of the project and its function
- Third sentence:
  - Explain the reason the program is being created and why the PIA is required





# PIA: Overview (of the program)

## The Overview Section:

- Creates the foundation for the entire PIA
- Provides the context and background necessary to understand the project's purpose and mission and the justification for operating a privacy sensitive project



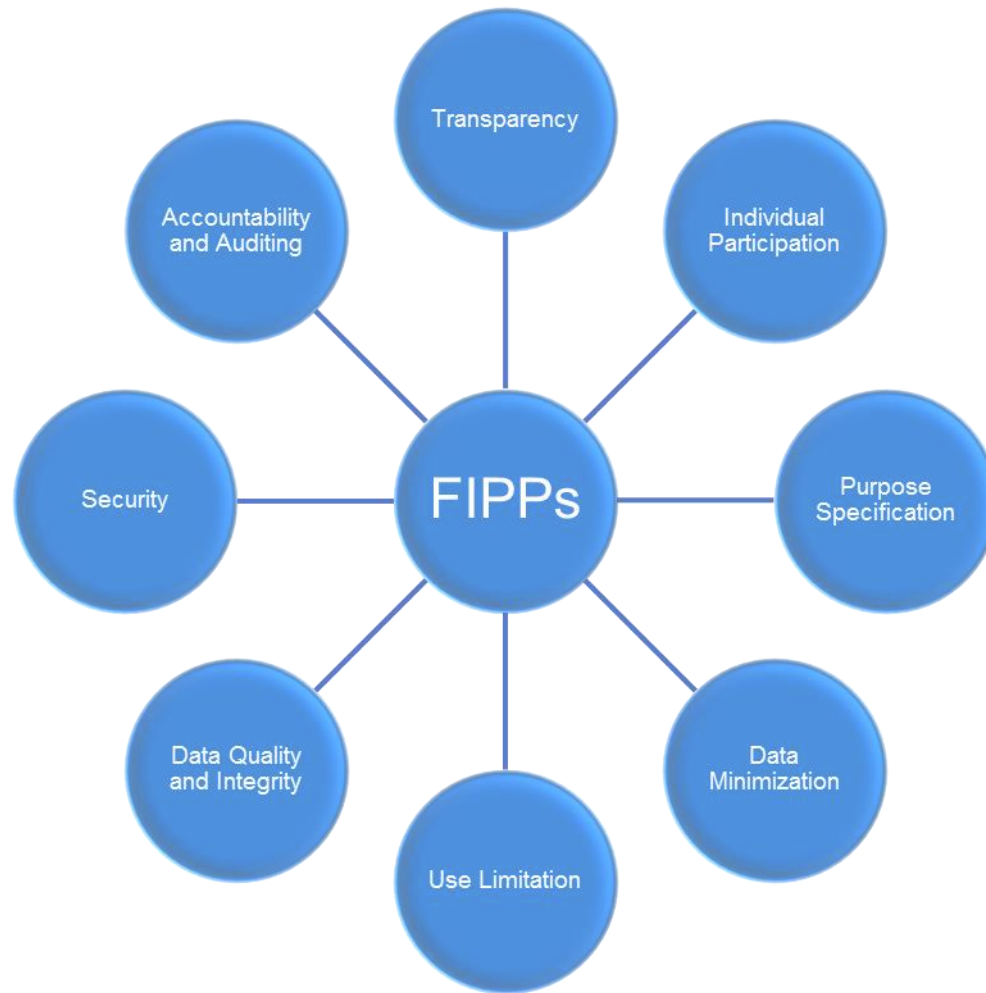
# PIA: Overview (continued)

The Overview Section includes the following:

- The purpose of the system, the name of the Department component(s) who own(s) or is funding the project
- Describe how and why the system collects and uses PII
- Typical transaction
- The recommendation for how the program has taken steps to protect privacy risk and mitigate risks ( in a holistic view)



# PIAs and the FIPPS



**Homeland  
Security**

| Privacy Office

# PIA Body: The FIPPS

- Section 1.0 Authorities and Other Requirements
  - Purpose Specification
- Section 2.0 Characterization of the Information
  - Purpose Specification
  - Data Minimization
  - Individual Participation
  - Data Quality and Integrity
- Section 3.0 Uses of the Information
  - Use Limitation
  - Transparency
- Section 4.0 Notice
  - Transparency
  - Use Limitation
  - Individual participation



# PIA Body: The FIPPS

- Section 5.0 Data Retention by the Project
  - Data Minimization
  - Data Quality and Integrity
  - Security
- Section 6.0 Information Sharing
  - Use Limitation
  - Security
- Section 7.0 Redress
  - Individual Participation
- Section 8.0 Auditing and Accountability
  - Accountability and Auditing



# Resources

Visit [www.dhs.gov/privacy](http://www.dhs.gov/privacy)  
for:

- Published PIAs
- Templates and Guidance:
  - PTA
  - PIA
  - SORN
  - NPRM/Final Rule
  - Privacy Act Statement
- Privacy Policy Guidance Memoranda



**Homeland  
Security**

| Privacy Office



# Homeland Security



**Homeland  
Security**

Privacy Office

Protecting privacy while promoting transparency



# ***System of Records Notices (SORN) and Privacy Act Statements***

Akbar Siddiqui  
Attorney-Advisor  
CBP

---

Elizabeth Doyle  
Attorney-Advisor,  
CBP



# System of Records Notice

Elizabeth C. Doyle

Akbar A. Siddiqui

June 10, 2014



U.S. Customs and  
Border Protection

# Why the SORN matters



Official White House Photo by Pete Souza



U.S. Customs and  
Border Protection

# Technology



Courtesy of the Library of Congress,  
LC-DIG-ggbain-09131; HAER CO-87-N-10

# The HEW Report

“Records, Computer, and the Rights of Citizens: Report of the Secretary’s Advisory Committee on Automated Personal Data Systems”



Courtesy of Library of Congress, LC-DIG-fsac-1a35456

# Privacy Act



Courtesy of U.S. National Archives, Series: Master Print File, compiled 1969-1974 (Collection RN-WHPO)

# Privacy Act

- Agencies must not disclose system records without written consent,
  - Exceptions
- Agencies must allow individuals to access and amend their records
- Agencies must publish rules that state which systems are exempt from access, amendment, or other requirements
- Agencies must account for disclosures
- Agencies must give notice to individuals
- Civil remedies
- Criminal penalties



# Do we need a SORN?

In general, Privacy Act applies to agency systems of records about individuals

- “Individual”: U.S. citizen or lawfully admitted alien (DHS policy includes non-resident aliens in mixed systems)
- “Record”: any item, collection, or grouping of information about an individual
- “System of records”: group of agency-controlled records from which information is retrieved (not merely “retrievable”) by name or other personal identifier

# SORN Guidance Online

- <http://www.dhs.gov/publication/system-records-notice-template>
- [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_nprm\\_template.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_nprm_template.pdf)
- [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_finalrule\\_template.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_finalrule_template.pdf)
- <http://www.dhs.gov/system-records-notices-sorns>
- <http://www.justice.gov/opcl/privacyact1974.htm>
- <http://www.justice.gov/opcl/prr.htm>



# Summary

- About 3-4 sentences
- Concise description of what system does
- May include reference to legacy SORN being updated

# Supplementary Information

- Two Parts
  - Background (about the system)
  - Privacy Act

# System of Records

- Beginning of the formal notice
- Official name of the system

# Categories of Individuals

- Be specific
- Include all individuals covered

# Categories of Records

- Call out sensitive information such as SSN, Biometrics
- Consistent with records' sources and how information retrieved
- Specific v. General

# Purpose

- Very important
- Why was this system of records created?

# Routine Uses

- Who is the information shared with?
- Not just “routine” but any sharing

# Standard Routine Uses

- Department of Justice for ongoing litigation
- Congress
- NARA
- Auditing and oversight (GAO, OMB)
- Law enforcement investigating a possible violation of law
- Contractors
- Identity theft



# Retrievability

- What information is retrievable?
- List should match ‘categories of records’ or be very similar

# Retention and Disposal

- Very important
- For how long?
- Why?

# Disclosure and Redress

- Notification Procedure
- Record Access Procedure
- Contesting Record Procedures

# Record Sources

- From individuals?
- Other DHS systems?
- Other Federal systems?
- Commercial systems?
- Consistent with Categories of Records

# Exemptions

- 5 USC § 552a(j)
- 5 USC § 552a(k)

# Exemptions

- 5 USC § 552a(j)(1)
  - Records maintained by the CIA
- 5 USC § 552a(j)(2)
  - Law enforcement
  - “Records maintained by an agency or component which performs as its principal function any activity pertaining to the enforcement of criminal laws and which consists of identifying data compiled for the purpose of a criminal investigation, associated with an identifiable individual: or reports identifiable to an individual compiled at any stage of the process of enforcement of criminal laws”

# Exemptions

- 5 USC § 552a(k)(1)
  - Classified material
  - “Relate to the national defense or foreign policy and are properly classified”
- 5 USC § 552a(k)(2)
  - Non-law enforcement but investigative
  - Must give access if denied Federal benefit
  - “Are investigatory and compiled for law enforcement purposes”

# Exemptions

- 5 USC § 552a(k)(3)
  - Presidential protection
  - “Pertain to the protection of the President of the United States”
- 5 USC § 552a(k)(4)
  - Statistical records
  - “Are required by statute to be maintained and used solely as statistical records”



# Exemptions

- 5 USC § 552a(k)(5)
  - Background checks and suitability
  - “Are investigatory and used for employee or contractor suitability determinations”
- 5 USC § 552a(k)(6)
  - Federal exams
  - “Are Federal service exam or test materials”
- 5 USC § 552a(k)(7)
  - Military promotions
  - “Are armed services promotion evaluation materials”

# Process before publication

- Internal review and approval
- Congress
- OMB
  - 10 calendar days to comment
- Federal Register
  - If no exemptions, effective 30 calendar days after publication

# Exemption Process

- Notice of Proposed Rulemaking (NPRM)
  - Initial notice to the public through the Federal Register
  - 30 day public comment period
  - Public comments pulled from [www.regulations.gov](http://www.regulations.gov)
  - All public comments that relate to the proposed rule must be addressed in the Final Rule or by amending the compliance documents
- Final Rule
  - Final notice to the public
  - All public comments received from [www.regulations.gov](http://www.regulations.gov) that relate to the proposed rule must be addressed

# Privacy Act Statement Examples

**Elizabeth C. Doyle**  
**Akbar A. Siddiqui**  
**June 10, 2014**



U.S. Customs and  
Border Protection

Last/Surname: 

First (Given) Name: 

Birth Date: 

Year (YYYY):

Month:


Day (DD):

Passport Number: 

Country of Issuance: 

Get Most Recent I-94

Get Travel History

 Note: For security reasons, we recommend that you close your browser after you have finished retrieving your I-94 number.

An agency may not conduct or sponsor an information collection and a person is not required to respond to this information unless it displays a current valid OMB control number. The control number for this collection is 1651-0111. The estimated average time to complete this application is 4 minutes. If you have any comments regarding the burden estimate you can write to U.S. Customs and Border Protection, Office of Regulations and Rulings, 90 K Street, NE, Washington DC 20229.

#### Privacy Act Statement

Pursuant to 5 U.S.C. § 552a(e)(3), this Privacy Act Statement serves to inform you of the following concerning the collection of the information on this form.

**AUTHORITIES:** The authorities supporting CBP's collection and use of the Form I-94/I-94W data include, The Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, codified in 50 U.S.C. §§ 401 et seq.; The Immigration and Nationality Act, 8 U.S.C. §§ 1101 et seq.; and the Homeland Security Act of 2002, 6 U.S.C. §§ 101 et seq.

**PURPOSE:** The information that you submit when attempting to access this website will be used to retrieve your arrival and departure records from the Non-Immigrant Information System (NIIS) collected during the preceding five years. CBP will retain the information you submit when attempting to access your records through this website for 3 months for audit and system performance purposes. NIIS maintains information for entry screening and admissibility determination purposes for nonimmigrant visitors to the United States. NIIS also serves to track the period of admissibility of nonimmigrant aliens and maintain a central repository of contact information for these aliens. It captures arrival and departure information to identify travel patterns, arrivals without departure, and nonimmigrant aliens overstaying their admissible terms in the United States. The timely and accurate capturing of this data is necessary for monitoring compliance with U.S. law.

**ROUTINE USES:** The information you submit for purposes of accessing this website will not be shared with any entities or persons outside of DHS. The information maintained in NIIS may be shared with other authorities to assist in determining your eligibility for a requested benefit, future admissibility, and in accordance with the approved routine uses described in the associated systems of records notices.

**DISCLOSURE:** The information you provide for purposes of accessing this website is voluntary. However, failure to provide all or any part of the information requested by DHS, or the provision of inaccurate information, may result in denial of access to this website.

[For inquiries or questions regarding your I-94, please click here.](#)

[Accessibility](#) | [Privacy Policy](#)

# Drafting a Privacy Act Statement

- Authority
- Purpose
- Routine Uses
- Effect of Disclosure
- Special Issues

# Review System and its SORN

The screenshot shows a web browser window with the address bar displaying <http://iprs.cbp.gov/>. The browser's address bar also shows a search icon, a refresh icon, and a tab titled "Intellectual Property...". The browser's toolbar includes a "Convert" button and a "Select" button. The website's header features the U.S. Customs and Border Protection logo, the text "U.S. Customs and Border Protection" and "Securing America's Borders", and the "DHS.gov" link. Below the header is a search bar with the text "IPRS INTELLECTUAL PROPERTY RIGHTS SEARCH" and a "Keyword" input field with a "GO" button. To the right of the search bar are links for "HELP", "ABOUT", and "PRINT". Below the search bar is a row of buttons for "Search", "ALL", "Title", "Product", "Description", "Owner", "Contact Name", "Firm Name", "Recordation No.", and "Agency Registration No.". Below this row is a "Filter" button and a row of buttons for "Show All", "Trademarks", "Copyrights", "Tradenames", "Exclusion Orders", "Exclude Expired", and "Include Expired". The main content area has a section titled "What's New" with the text "The total number of searchable IPR recordations in this database is 32049." Below this is a section titled "About the Intellectual Property Rights Search (IPRS)" with a paragraph explaining the database and its search capabilities. A note box states: "Note: The IPRS database is updated nightly (except Saturday and Sunday) at approx. 4:00 a.m. eastern standard time. Those basing import/exports transactions based upon data contained within IPRS are reminded that recordation information is updated by CBP IPR Branch personnel daily." Below the note is a section titled "Related IPRS Information" with a link to "U.S Customs & Border Protection (CBP) IPR Enforcement". At the bottom, a footer text says "Please submit any technical concerns related to IPRS to [CBP website technical questions](#)."

http://iprs.cbp.gov/

Intellectual Property...

Convert Select

U.S. Customs and Border Protection  
Securing America's Borders

DHS.gov

IPRS INTELLECTUAL PROPERTY RIGHTS SEARCH

Keyword  GO

HELP | ABOUT | PRINT

Search ALL Title Product Description Owner Contact Name Firm Name Recordation No. Agency Registration No.

Filter Show All Trademarks Copyrights Tradenames Exclusion Orders Exclude Expired Include Expired

### What's New

The total number of searchable IPR recordations in this database is 32049.

### About the Intellectual Property Rights Search (IPRS)

IPRS is a searchable database containing public versions of U.S. Customs and Border Protection intellectual property rights recordations. Recordations can be retrieved based on simple or complex search characteristics using keywords and Boolean operators. IPRS has the added functionality of restricting searches to specific fields and record types. IPRS contains expired as well as current records and by default excludes expired records. For more information about features or how to use IPRS, please visit the [HELP section](#).

**Note:** The IPRS database is updated nightly (except Saturday and Sunday) at approx. 4:00 a.m. eastern standard time. Those basing import/exports transactions based upon data contained within IPRS are reminded that recordation information is updated by CBP IPR Branch personnel daily.

### Related IPRS Information

[U.S Customs & Border Protection \(CBP\) IPR Enforcement](#)

Please submit any technical concerns related to IPRS to [CBP website technical questions](#).

# Privacy Act Statement

- **Authority:** 15 U.S.C. § 1124; 17 U.S.C. §§ 101, 602-603; and 19 U.S.C. §§ 1526, 1595a, and 1624, as well as 31 U.S.C. § 9701, 19 C.F.R. §§ 133.3, 133.13, and 133.33.
- **Purpose:** CBP will use this information to identify infringing articles at the borders and prevent the importation of counterfeit or pirated merchandise.



# Privacy Act Statement

- **Routine Uses:** The indicated information on the public facing website, <http://iprs.cbp.gov/> will assist the public in ensuring it purchases non-infringing merchandise. CBP will use all the information to assist in the enforcement of intellectual property rights; CBP may share the information with other DHS components or other appropriate government agencies, consistent with the routine uses outlined in: Privacy Act of 1974; U.S. Customs and Border Protection; DHS/CBP-004-Intellectual Property Rights e-Recordation and Search Systems, System of Records, 78 F. R. 3015 (Jan. 15, 2013).
- **Disclosure:** Furnishing this information is voluntary; however, failure to furnish the requested information may delay CBP or prevent the public from identifying merchandise that infringes upon your intellectual property rights.



# U.S. Customs and Border Protection

## Our Mission

We are the guardians of our Nation's borders.

We are America's frontline.

We safeguard the American homeland at and beyond our borders.

We protect the American public against terrorists and the instruments of terror.

We steadfastly enforce the laws of the United States while fostering our nation's economic security through lawful international trade and travel.

We serve the American public with vigilance, integrity and professionalism.



Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



# ***Unmanned Aircraft Systems (UAS)***

Scott Mathews  
Acting Director  
DHS Privacy Office



Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



# ***Disruptive Technologies and Privacy***

Christopher S. Lee, J.D., CIPP/G

DHS S&T Privacy Officer

Christopher.Lee@hq.dhs.gov

# ***Overview***

- **Wearable Technologies**
- **Insider Threats**
- **Open Data, Big Data & All Things Internet**





# Wearable Technologies



**Homeland  
Security**

| Privacy Office

# ***Wearable Technologies Privacy Risks***

- First Amendment Freedom of Speech
- Fourth Amendment Unreasonable Search & Seizure
- Anti-Wiretapping Laws
- Fair Information Practice Principles
  - Transparency, Notice & Disclosure
  - Use Limitation
  - Purpose Specification
  - Security
  - Accountability and Auditability



# Insider Threats

## The Washington Post

### FDA says it monitored workers' e-mail to investigate potential leak

By [Ellen Nakashima](#) and [Lisa Rein](#), Published: February 9, 2012

The Food and Drug Administration said Thursday that it monitored the personal e-mails of employees who had concerns about unsafe medical devices beginning in April 2010 but said it did so to investigate allegations that the employees had leaked confidential information to the public.

## Los Angeles Times | ARTICLE COLLECTIONS

### Shootout between federal agents kills 1, wounds 1

*The shooting in the Glenn M. Anderson Federal Building in Long Beach reportedly involved a dispute between an Immigration and Customs Enforcement agent and his supervisor. The agent shot his boss and then was killed by another agent.*

February 17, 2012 | By Andrew Blankstein, Robert J. Lopez and Ruben Vives, Los Angeles Times

A confrontation between federal law enforcement agents erupted in gunfire Thursday evening in Long Beach, leaving one dead and another seriously injured, authorities said.



**Homeland  
Security**

| Privacy Office



# Insider Threats



Homeland  
Security

Privacy Office

# ***Insider Threat Privacy Risks***

- First Amendment Freedom of Speech
- Fourth Amendment Unreasonable Search & Seizure
- Protected Communications
  - Classified Documents & Discussions
  - Attorney/Client Privilege
  - Doctor/Patient Privilege
  - Medical Records
  - Employee Performance Plans
  - Whistle Blower Protection Act



# Open Data, Big Data & All Things Internet



The White House

Office of the Press Secretary

[E-Mail](#) [Tweet](#) [Share](#) [+](#)

For Immediate Release

May 09, 2013

## **Executive Order -- Making Open and Machine Readable the New Default for Government Information**

EXECUTIVE ORDER

-----

MAKING OPEN AND MACHINE READABLE THE NEW DEFAULT  
FOR GOVERNMENT INFORMATION



**Homeland  
Security**

| Privacy Office



# Re-identification



- 2007 Netflix released anonymized data sets containing customer viewing habits, and challenged researchers to improve movie recommendations algorithms. The winner received a \$1 million prize.
- Researchers from the University of Texas were able to re-identify individual users by matching the data sets with film ratings on IMDB.
- 2009 four Netflix users filed a class action lawsuit against Netflix, alleging that Netflix had violated the Video Privacy Protection Act by releasing the data sets.
- 2010 the case was settled out of court.

[http://en.wikipedia.org/wiki/Netflix\\_Prize](http://en.wikipedia.org/wiki/Netflix_Prize)



**Homeland  
Security**

| Privacy Office

# ***De-Identifying Protected Health Information (PHI)***

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code or equivalents except for the initial 3 digits of a zip code if the corresponding zone contains more than 20,000 people.
3. All elements of dates (except year) for dates directly related to the individual (birth date, admission date, discharge date, date of death). Also all ages over 89 or elements of dates indicating such an age.
4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan numbers
10. Account numbers
11. Certificate or license numbers
12. Vehicle identification or serial numbers including license plate numbers
13. Device identification or serial numbers
14. Universal resource locators (URL's)
15. Internet Protocol addresses (IP addresses)
16. Biometric identifiers
17. Full face photographs and comparable images
18. Any other unique identifying number, characteristic, or code

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html>



**Homeland  
Security**

| Privacy Office

# ***Open Data & Big Data Privacy Risks***

- Re-identification
- Use Limitation
- Purpose Specification
- Data Sharing

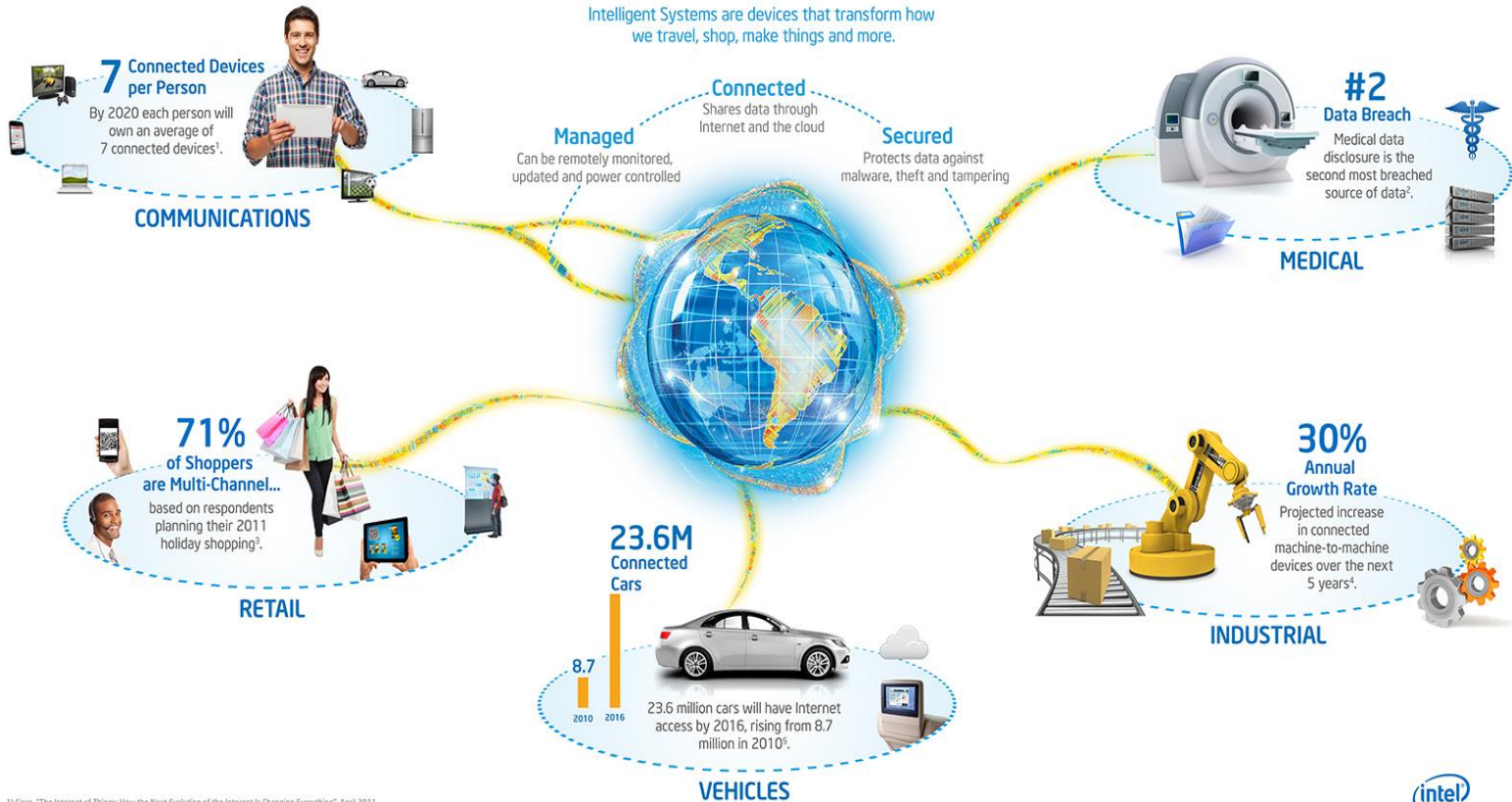


# Internet of Things

## Intelligent Systems for a More Connected World

### WHAT ARE INTELLIGENT SYSTEMS?

Intelligent Systems are devices that transform how we travel, shop, make things and more.



<sup>1</sup>) Cisco, "The Internet of Things: How the Next Evolution of the Internet is Changing Everything", April 2011  
<sup>2</sup>) Bloomberg Research, "Security challenges in the US healthcare sector" White Paper, December 2010, <http://www.bloombergr.com/resources/white-papers/wp-bloom-healthcare-security.pdf>  
<sup>3</sup>) Deloitte U.S., 2011 Annual Holiday Survey, [http://www.deloitte.com/assets/Doc-United-States/Local/20Assets/Documents/Consumer%20Business/us\\_retail\\_AnnualHolidaySurvey\\_2011\\_pr\\_102611.pdf](http://www.deloitte.com/assets/Doc-United-States/Local/20Assets/Documents/Consumer%20Business/us_retail_AnnualHolidaySurvey_2011_pr_102611.pdf)  
<sup>4</sup>) McKinsey Global Institute analysis, "Big data: The next frontier for innovation, competition, and productivity", June 2011  
<sup>5</sup>) Wall Street Journal, <http://online.wsj.com/article/SB100014240665945763497631493384.html>, estimate from research firm, Frost & Sullivan

<sup>6</sup>) 2013 Intel Corporation. All rights reserved. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries. \*Other names and brands may be claimed as the property of others.



**Homeland  
Security**

Privacy Office





Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



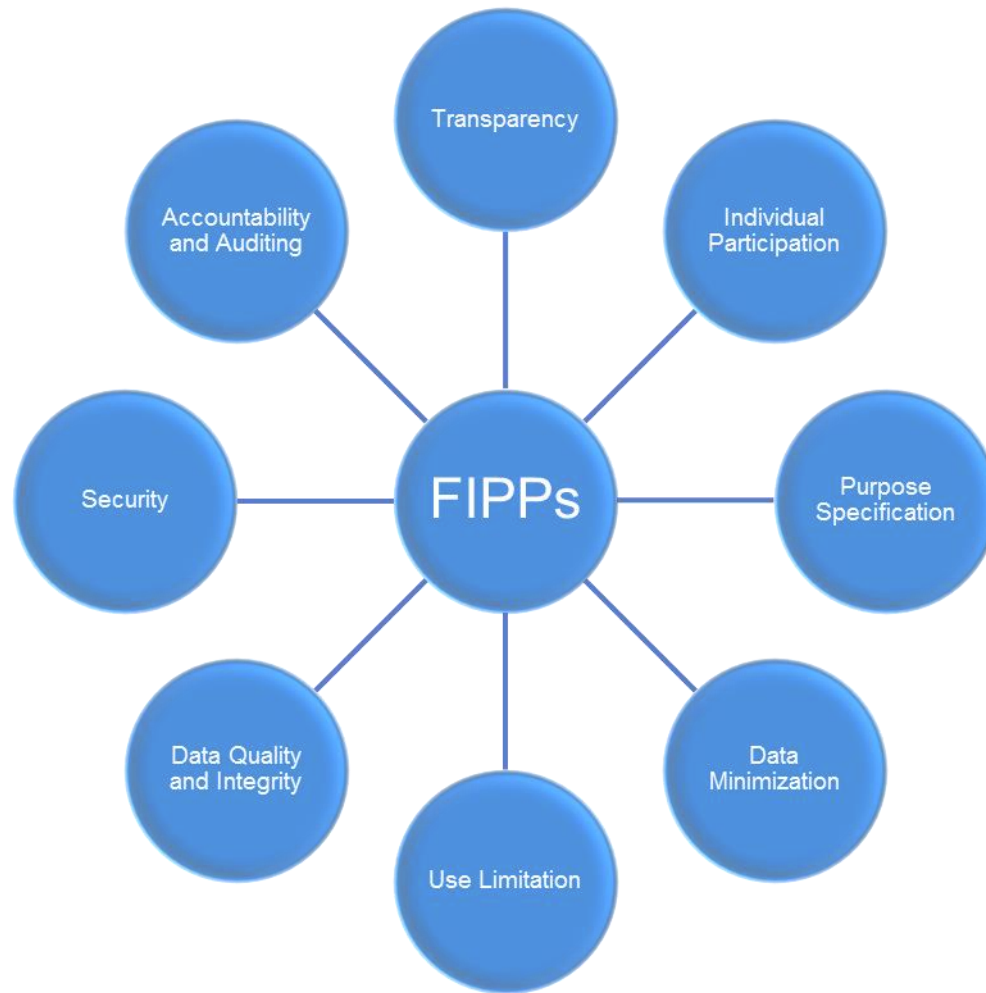
# Homeland Security

---

## Science and Technology



# The FIPPS





Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



# *Identity Management Foundations for Government Privacy Professionals*

2014 DHS Privacy Office Annual Compliance Workshop

Anil John, FICAM Trust Framework Solutions PM, GSA

Jamie Danker, Verification Privacy Officer, Office of Privacy, U.S.  
Citizenship and Immigration Services

Dawn Wiggins, Deputy Executive Director, Office of Privacy &  
Disclosure, Social Security Administration

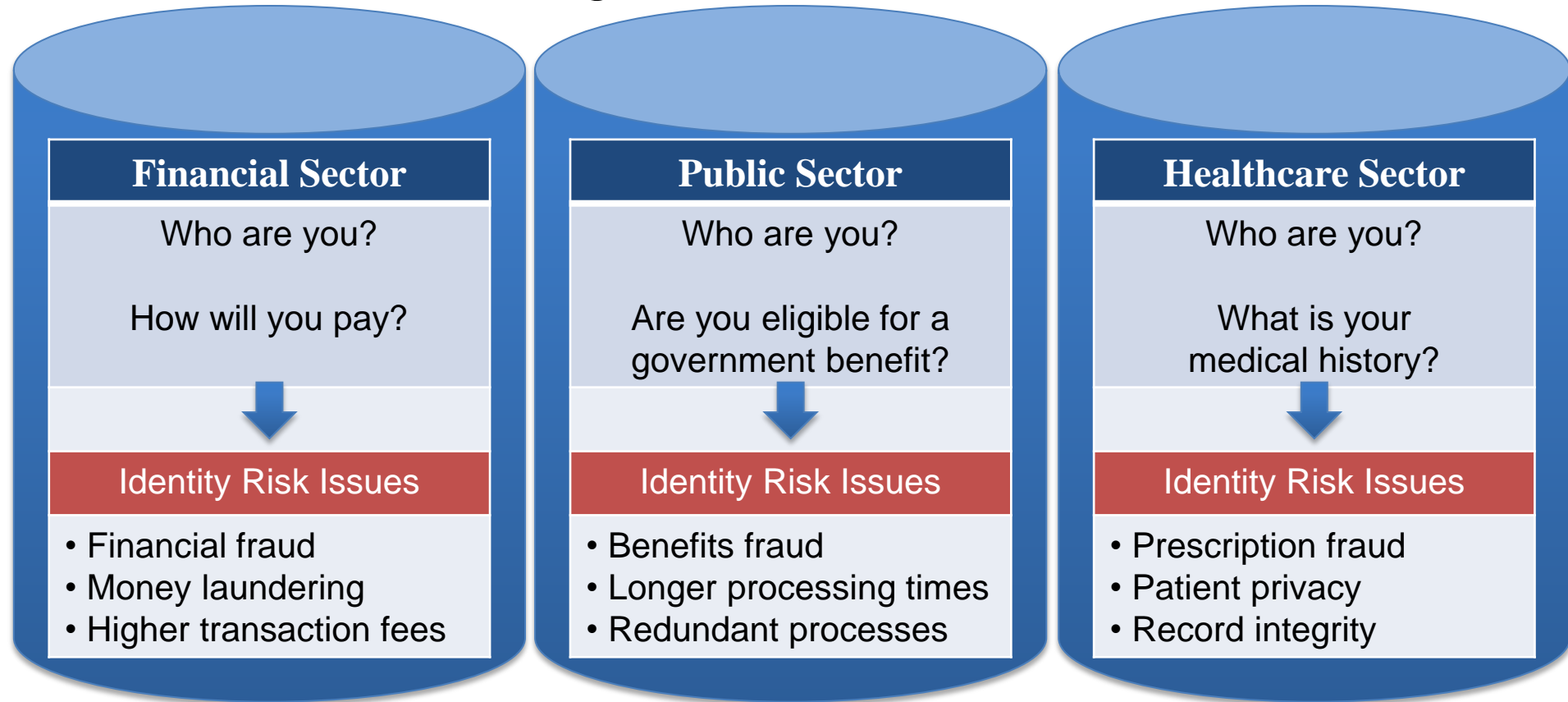
# *Agenda*

- Identity Management Basics
- Citizen-centered Agency Use Cases
  - E-Verify Self Check (USCIS)
  - mySSA (Social Security Administration)
- Interactive Exercise
- Q&A



# Identity is the Starting Point for Online Delivery of High Value Services, Benefits and Entitlements

Today, identity is managed in “cylinders of excellence” a.k.a silos ...



... but the impacts are felt by everyone



# Impact of un-mitigated Identity Risk

- Inconvenience, distress or damage to standing or reputation
- Financial loss or organization liability
- Harm to an organization's programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

December 16, 2003

M-04-04

MEMORANDUM TO THE HEADS OF ALL DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten  
Director

SUBJECT: E-Authentication Guidance for Federal Agencies

The Administration is committed to reducing the burden on businesses, and improving government response time. To achieve these goals, citizens need to be able to interact with the government by using the Internet. This guidance document provides information on how to accomplish using the Internet online. It also provides information on how government services are secure and how authentication is needed.

The attached guidance, "E-Authentication Guidance for Federal Agencies," is the result of the E-Government Act of 2002. The guidance is the result of the E-Authentication Institute of Standards and Technology (E-AUTH) working closely with and incorporating the views of the public.

The guidance covers the area of authentication (or e-authentication) and a need for government-wide standards for authentication needs for electronic transactions. It also provides information on how to conduct "e-authentication risk assessments" on electronic transactions. It provides a consistent approach across government. (See Attachment B for more information on the criteria for access to Federal government services.) Attachment B summarizes the public comments received on an earlier version of the guidance.

For any questions about this guidance, contact Jeanette Thornton, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3562, fax (202) 395-5167, e-mail: [eaauth@omb.eop.gov](mailto:eaauth@omb.eop.gov).

Attachments

Attachment A – E-Authentication Guidance for Federal Agencies  
Attachment B – Summary of Public Comments and Responses

OMB 04-04

# Level of Assurance = Confidence in Identity

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or organization liability	Low	Mod	Mod	High
Harm to an organization's programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High
<b>Needed Level of Assurance →</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>

# Level of Assurance – A Worked Example

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or organization liability	Low	Mod	Mod	High
Harm to an organization's programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High
<b>Needed Level of Assurance →</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>



# Unauthorized release of sensitive personal or commercial information

## Level 1

- N/A

## Level 2

- A **limited adverse effect** on an individual or institution due to the loss of confidentiality or breach of privacy resulting from unauthorized release or improper disclosure of sensitive personal or commercial information

## Level 3

- A **serious effect** on an individual or institution due to the loss of confidentiality or breach of privacy resulting from unauthorized release or improper disclosure of sensitive personal or commercial information

## Level 4

- A **catastrophic effect** on an individual or institution due to the loss of confidentiality or breach of privacy resulting from unauthorized release or improper disclosure of sensitive personal or commercial information



# Unauthorized release of sensitive government information (non-personal information)

## Level 1

- N/A

## Level 2

- A **limited adverse effect** on organizational operations and assets due to a loss of confidentiality resulting from the release of government sensitive information to unauthorized parties

## Level 3

- A **serious effect** on organizational operations and assets due to a loss of confidentiality resulting from the release of government sensitive information to unauthorized parties

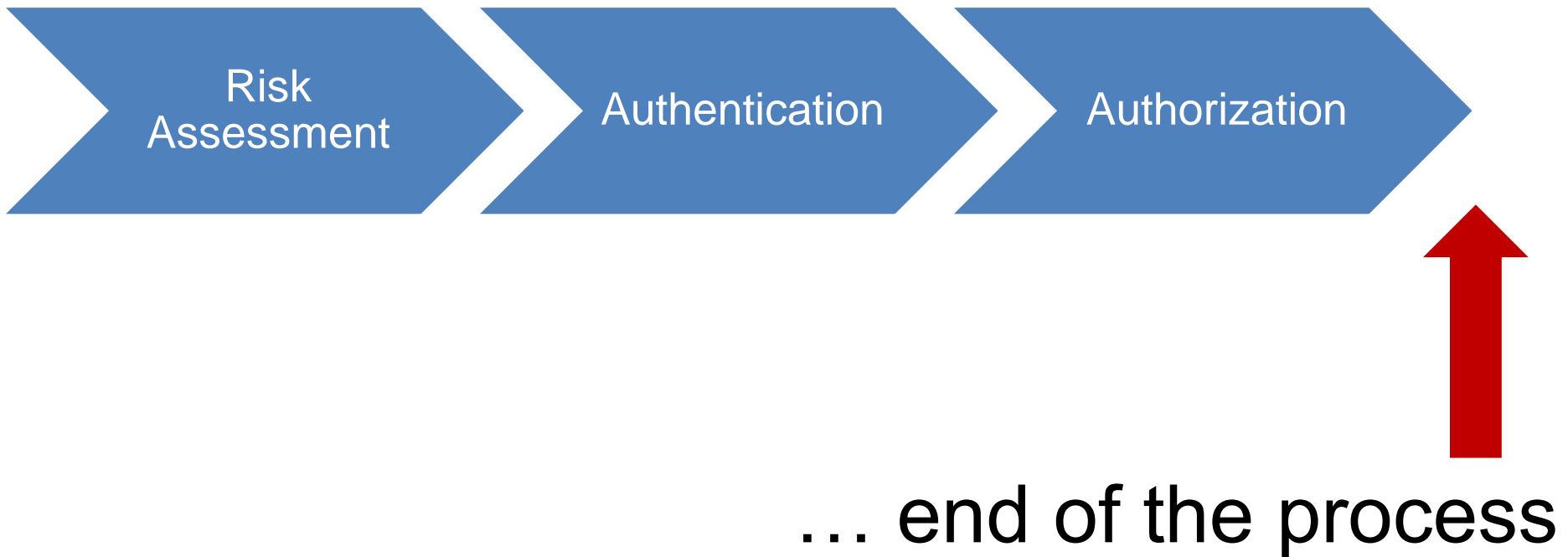
## Level 4

- A **catastrophic effect** on organizational operations and assets due to a loss of confidentiality resulting from the release of government sensitive information to unauthorized parties

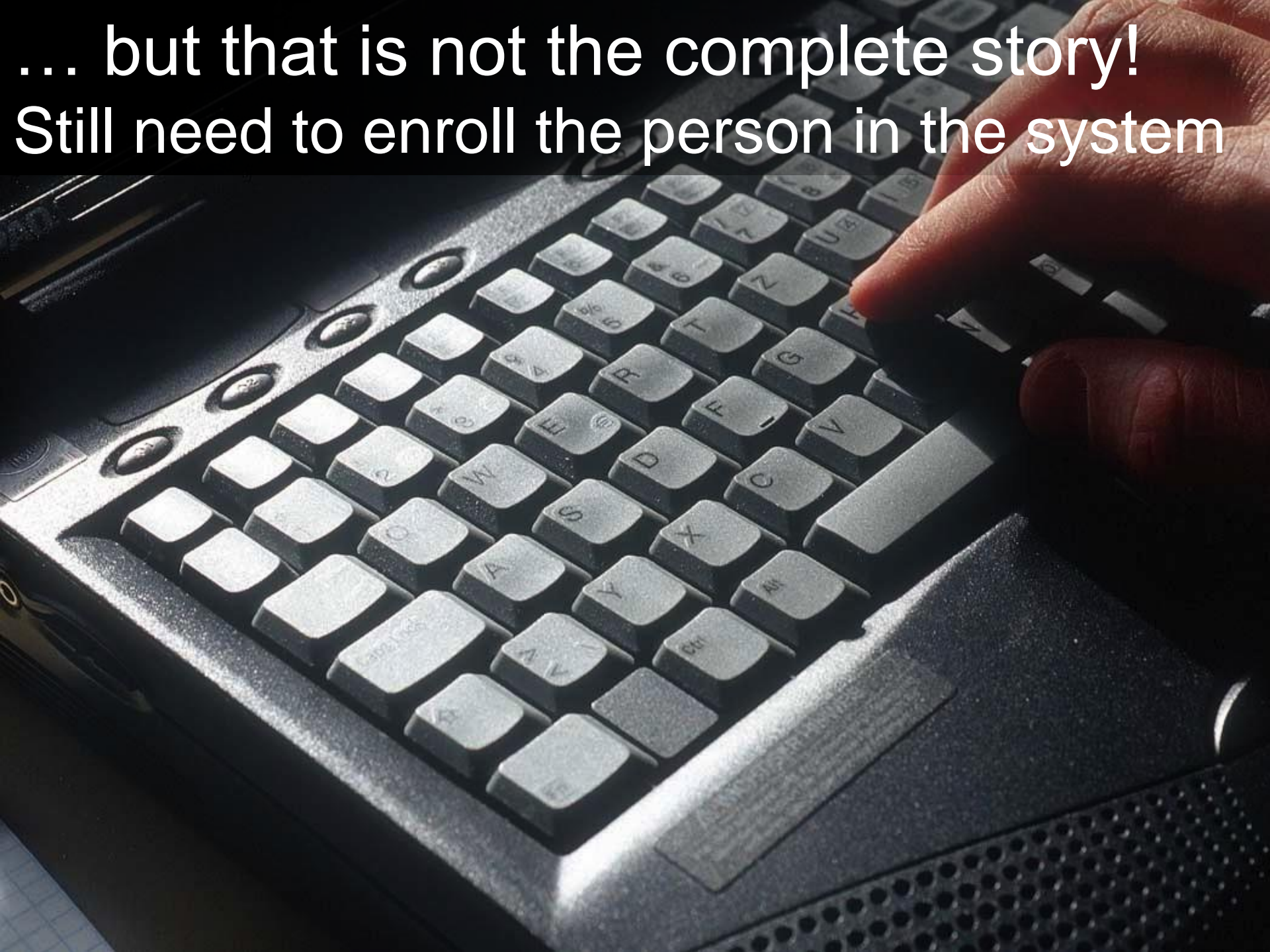
# Credentials that meet requirements for assurances of identity to mitigate risk

Credential Types	Identity Proofing	Level of Assurance			
		1	2	3	4
Weak Password & PINs	None	√			
Single-Factor Non-shared Password or Token	2 Docs / 1 Verified (May be remote)	√	√		
Multi-Factor Hard or Soft Crypto, OTP Token	2 Docs / 2 Verified (May be remote)	√	√	√	
Multi-Factor FIPS 140-2 Hard Crypto Token with Encryption	2 Gov Docs Verified In Person + Biometric Capture	√	√	√	√

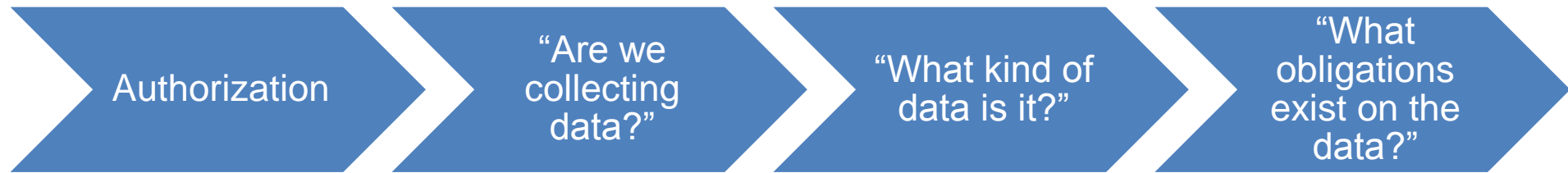
Identity and security people typically stop at this point since OMB-O4-04 ....



... but that is not the complete story!  
Still need to enroll the person in the system



# Enrollment means that for Privacy People there is incoming data...



... beginning of the process

# What do we need?

Are you the  
same  
person this  
credential  
was issued  
to?



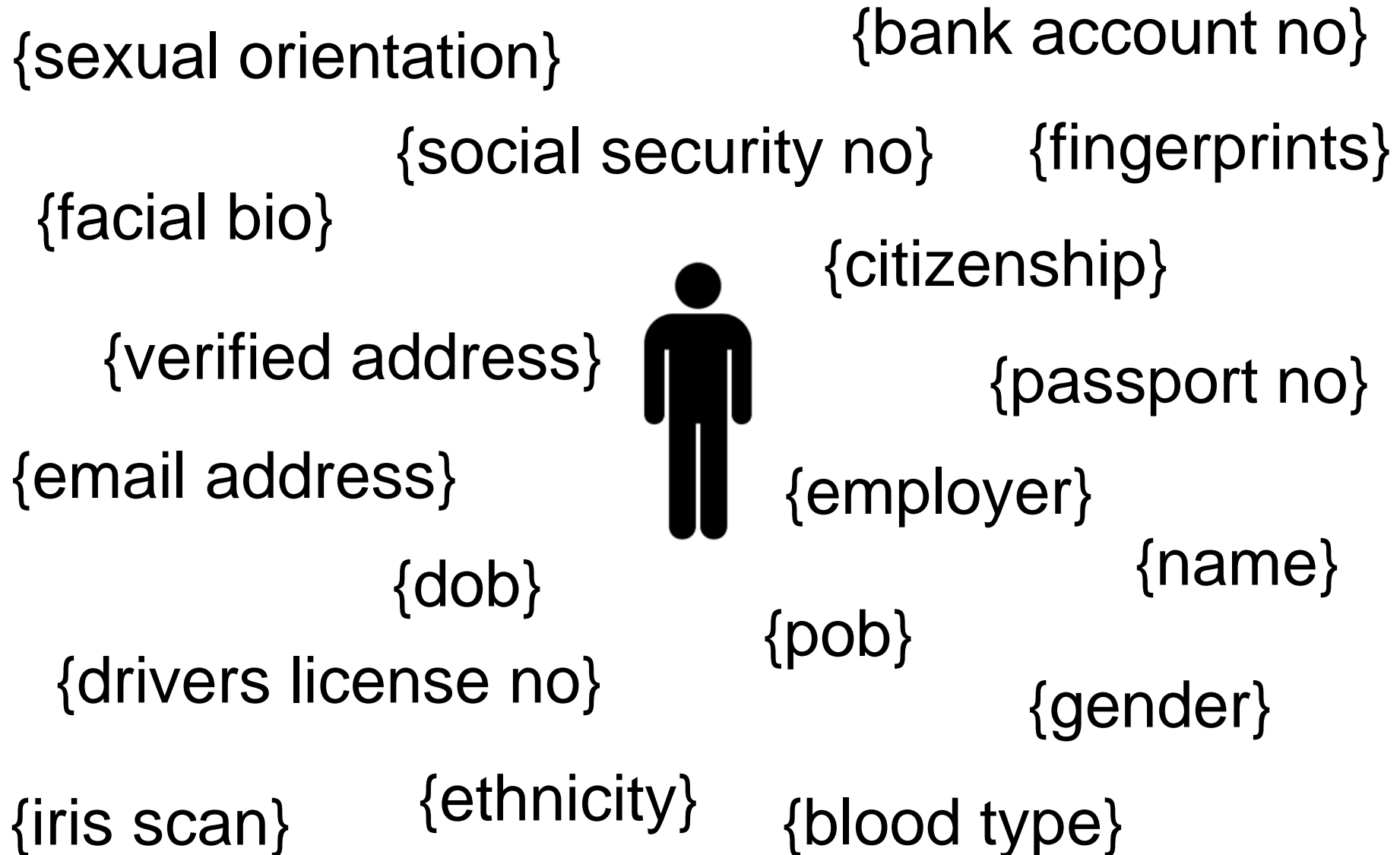
Standardized  
LOA 1- 4

??



Information  
to uniquely  
resolve and  
enroll the  
credential  
holder

# Enrollment requires Personally Identifiable Information to uniquely resolve a person



PII requested MUST balance privacy concerns and assurance needs while being cost-effective





There are no standards here...



# ... but Privacy is Critical to Services!

- **Fraud and security concerns** are inhibiting confidence, trust and growth of e-Government services
- **Fear of surveillance** and excessive collection, use and disclosure of identity information are diminishing confidence in and use of citizen facing services
- **Lack of citizen empowerment** and control over one's own personal data is diminishing confidence and use

*Any Citizen Facing Service MUST address these concerns to be credible and successful*

Disclosure of personal information to .gov  
must be minimal and contextually relevant





# ***LOA 2 Agency Example: Self Check***

- **2009:** Requested by Congress, Self Check is a voluntary, fast and free service that allows an **individual** to make sure the employment eligibility records used by E-Verify are up to date and accurate.
- **2011:** Self Check was launched in five states and D.C.
  - On August 15, 2011 the service was made available in Spanish and expanded to an additional 16 states.
  - On February 9, 2012 Self Check was made available nationwide.
- **2013:** Over 181,000 individuals have used Self Check since its launch.

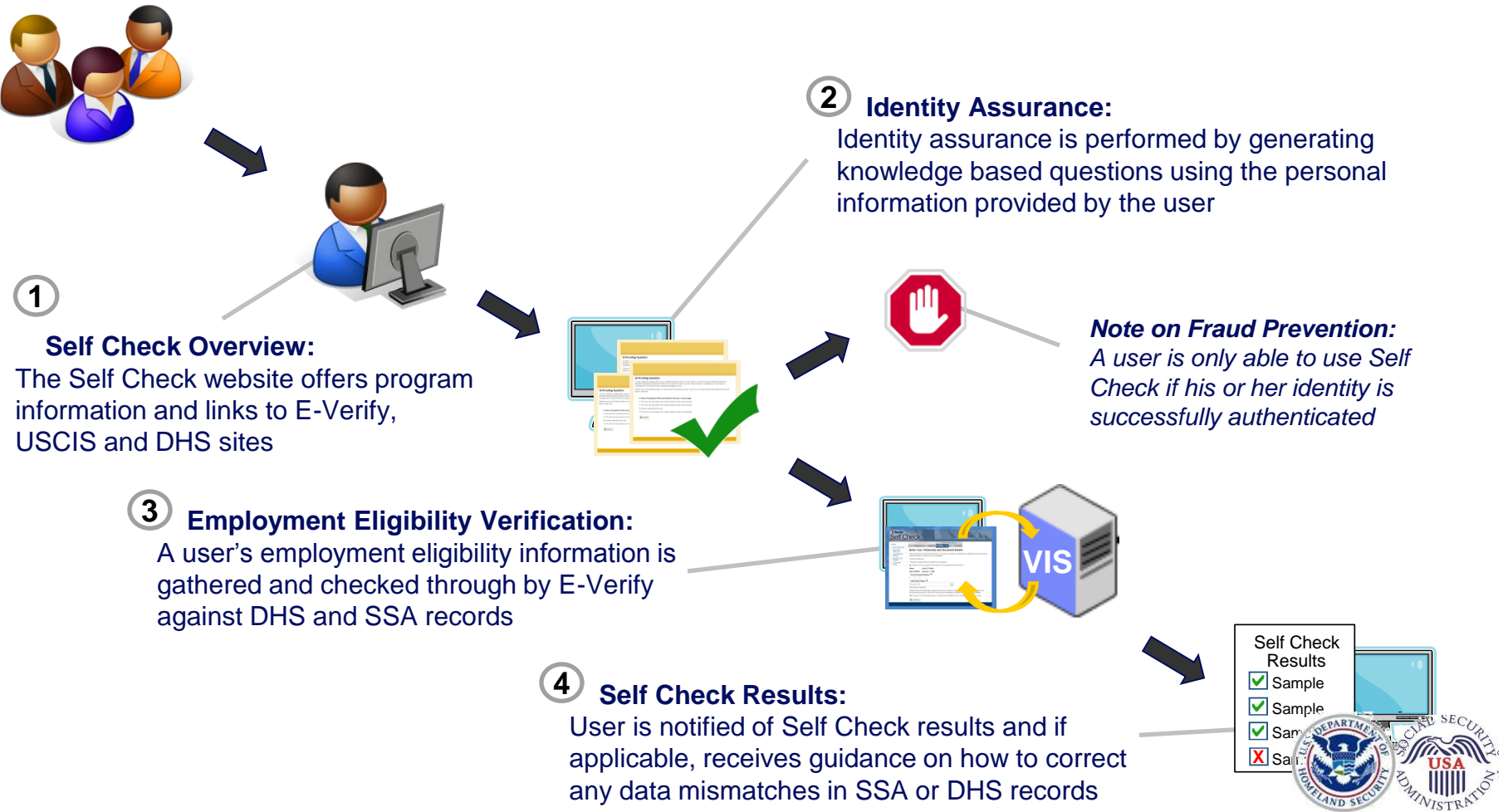


# ***E-Verify and Self Check Comparison***

	E-Verify Program	Self Check Service
<b>Audience</b>	U.S. businesses	U.S. workers
<b>Purpose</b>	Verify employment eligibility of workforce	Check your own employment eligibility status
<b>System Security</b>	Employer registration process and user accounts	Identity assurance process on each use
<b>Legislative Mandate</b>	Required in certain states and for federal contractors	Voluntary, cannot be required
<b>Availability</b>	50 states and U.S. territories	50 states and U.S. territories



# Self Check Process Overview



Homeland  
Security

Privacy Office

# User's View of the Self Check Process



## Step 1 - Enter ID Data

- Enter basic identifying information like name, address, date of birth, and Social Security number (SSN).
- Providing SSN is optional in Step 1. If not provided here, SSN will be required in Step 3.



# Self Check Terms of Use & Data Entry Screens

## Self Check

[Self Check Home](#)[About Self Check](#)[How To Use Self Check](#)[Know Your Rights](#)[Our Commitment To Privacy](#)[Questions And Answers](#)[For Employers](#)

### Self Check Terms of Use

[Ver en Español](#)

By accessing, viewing, or using Self Check, you are agreeing to use this service in compliance with the Terms of Use and Privacy Statement below and all applicable laws and regulations. To use the Self Check service, you must accept these terms of use by checking the box at the bottom of this page.

#### Terms of Use

##### Security

You are entering an official United States Government System, which may be used only for authorized purposes. Websites for the Department of Homeland Security (DHS) have been established in accordance with the Interim ISS Directive, which includes regular risk assessments and certifications. The Chief Information Officer of the Department of Homeland Security is the final authority on security requirements and controls for Homeland Security Websites. Every effort is made to ensure the quality, integrity and utility of the information on this site while ensuring privacy and security. Only authorized personnel may alter Web pages. Unauthorized use of this system is prohibited.

##### Privacy Statement

###### Our Privacy Commitment to You

U.S. Citizenship and Immigration Services (USCIS) is committed to maintaining the privacy of your Personally Identifiable Information (PII) in accordance with USCIS standards.

###### Your Expectation of Privacy

USCIS understands that you expect your privacy and personal information to be protected. That is why the Self Check service is designed to require that you authenticate your identity before we allow you to access the information we have about you.

☐ By clicking this box, the "Continue in English" or "Continuar en Español" button, and using this site, you agree to do so in compliance with these terms and conditions and all applicable laws and regulations. If you do not agree to these terms, you cannot use Self Check.

[Continue in English](#)[Continuar en Español](#)

U.S. Department of Homeland Security : dhs.gov U.S. Citizenship and Immigration Services : uscis.gov

Accessibility

## Self Check

[Self Check Home](#)[About Self Check](#)[How To Use Self Check](#)[Know Your Rights](#)[Our Commitment To Privacy](#)[Questions And Answers](#)[For Employers](#)[Cancel Self Check](#)

ESTABLISH IDENTITY

CONFIRM WORK ELIGIBILITY

1 Enter ID Data

2 Take a Quiz

3 Enter Document Data

4 Get Results

### Enter Your Identifying Information

The information that you enter below will be used by a third party identity assurance service to generate questions. Every Self Check user is required to answer these questions to ensure that an individual is only allowed to perform an employment eligibility check on his or her own records. The name and date of birth entered below will be "locked in" for use in the employment eligibility check later.

\*All fields marked with an asterisk are required.  
Please click any question mark icon below to view additional instructions.

Name :

\*First Name :

MI :

\*Last Name :

Date of Birth :

\*Year:

\*Month:

\*Day:

Social Security Number :

-  -

Address :

\*Street :

\*City :

\*State :

\*Zip Code :

Neither the Department of Homeland Security nor any component Agency or program will know the questions you are asked or the answers that you choose. In addition, all information entered above will be deleted from the Self Check system at the end of your session. Once we know from the identity authentication service that you have proven your identity, we are ready to let you query government databases and determine your work eligibility.

Details about the Self Check policy are located in the privacy statement found on the previous screen.

Please review the information above before proceeding.

[Continue](#)

U.S. Department of Homeland Security : dhs.gov U.S. Citizenship and Immigration Services : uscis.gov

Accessibility

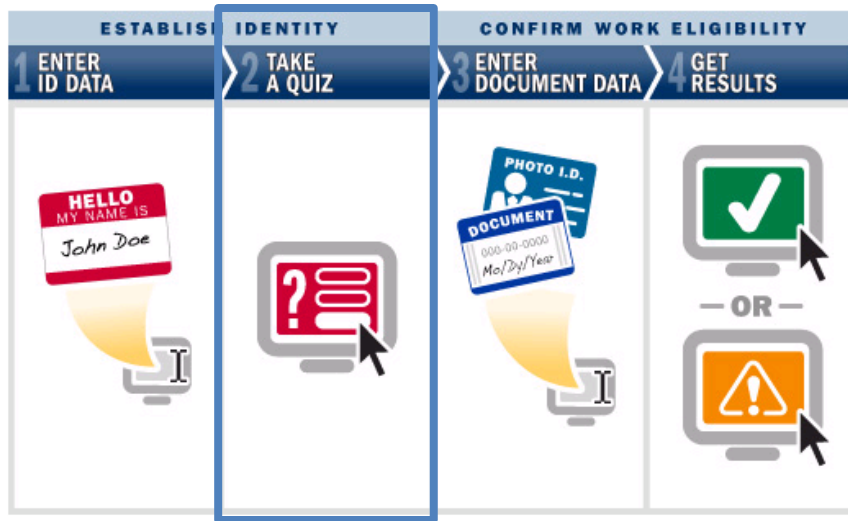


Homeland  
Security

Privacy Office



# User's View of the Self Check Process



## Step 2 - Take a Quiz

- The info is sent to a third party identity assurance service to generate a “quiz” for user to prove identity.
- The government will have no knowledge of which questions are presented or how those questions are answered.



# Identity Proofing Quiz

## ID Proofing Question

You are visiting an independent, secure, identity assurance service. This service is using non-governmental information to generate identity-based questions that only you should be able to answer. When the quiz is completed, you will return to complete the E-Verify Self Check employment eligibility check.

Please do not use the Back button on your browser during this process. If you do, your session will be terminated and you will have to start over.

**A series of questions will be presented to the user, one per page**

- ☐ The user can only select one of these options as the correct answer
- ☐ The user can only select one of these options as the correct answer
- ☒ Answer selected by the user
- ☐ The user can only select one of these options as the correct answer



**Homeland  
Security**

| Privacy Office

# User's View of the Self Check Process



## Step 3 – Enter Document Data

- If successful in Step 2, go on to complete an employment eligibility query to determine work eligibility.
- Additional required info includes SSN, citizenship status, and details from immigration documentation (e.g., Green card, EA card, etc).



# User's View of the Self Check Process



## Step 4 - Get Results

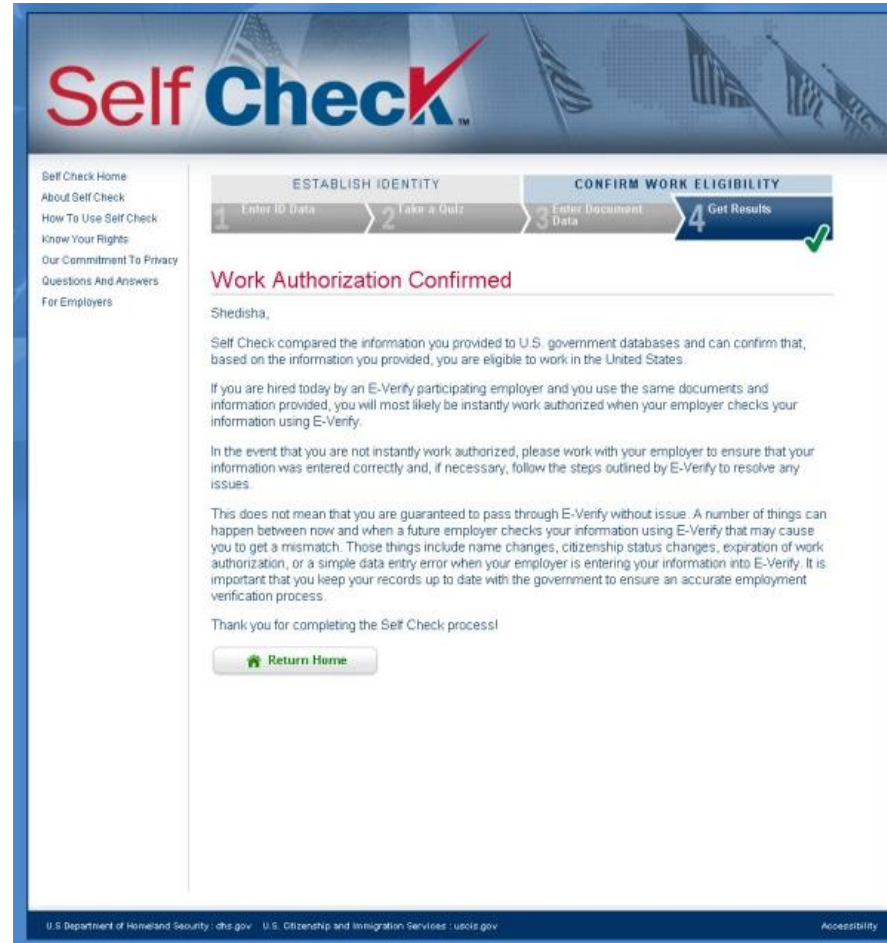
- Information submitted is checked against Department of Homeland Security (DHS) and Social Security Administration (SSA) databases to determine work eligibility.
- A response is given indicating either that the user would likely be employment authorized in E-Verify (if an employer runs the employment authorization check), or that there is a mismatch between the data entered and the DHS and/or SSA databases. If there is a mismatch, user will be given information that outlines how to correct the records if desired.



**Homeland  
Security**

| Privacy Office

# Employment Authorization Response Screen



The screenshot displays the 'Self Check' web interface. At the top, the 'Self Check' logo is prominently featured. Below it, a progress bar indicates four steps: 1. Enter ID Data, 2. Take a Quiz, 3. Enter Document Data, and 4. Get Results. Step 4 is currently active, marked with a green checkmark. The main content area is titled 'Work Authorization Confirmed' and addresses a user named 'Shedisha'. It provides a confirmation message stating that the user's information has been verified against U.S. government databases, confirming their eligibility to work in the United States. It also offers guidance on what to expect if hired by an E-Verify participating employer and provides instructions on how to resolve any issues that may arise. A 'Return Home' button is located at the bottom of the main content area. The footer of the page includes links to the U.S. Department of Homeland Security and U.S. Citizenship and Immigration Services, along with an 'Accessibility' link.

**Self Check**

Self Check Home  
About Self Check  
How To Use Self Check  
Know Your Rights  
Our Commitment To Privacy  
Questions And Answers  
For Employers

**ESTABLISH IDENTITY**      **CONFIRM WORK ELIGIBILITY**

1 Enter ID Data   2 Take a Quiz   3 Enter Document Data   4 Get Results ✓

### Work Authorization Confirmed

Shedisha,

Self Check compared the information you provided to U.S. government databases and can confirm that, based on the information you provided, you are eligible to work in the United States.

If you are hired today by an E-Verify participating employer and you use the same documents and information provided, you will most likely be instantly work authorized when your employer checks your information using E-Verify.

In the event that you are not instantly work authorized, please work with your employer to ensure that your information was entered correctly and, if necessary, follow the steps outlined by E-Verify to resolve any issues.

This does not mean that you are guaranteed to pass through E-Verify without issue. A number of things can happen between now and when a future employer checks your information using E-Verify that may cause you to get a mismatch. Those things include name changes, citizenship status changes, expiration of work authorization, or a simple data entry error when your employer is entering your information into E-Verify. It is important that you keep your records up to date with the government to ensure an accurate employment verification process.

Thank you for completing the Self Check process!

[Return Home](#)

U.S. Department of Homeland Security : dhs.gov   U.S. Citizenship and Immigration Services : uscis.gov   Accessibility



**Homeland  
Security**

| Privacy Office

# Possible Mismatch Screens

**Self Check**

Self Check Home  
About Self Check  
How To Use Self Check  
Know Your Rights  
Our Commitment To Privacy  
Questions And Answers  
For Employers

**ESTABLISH IDENTITY** 1 Enter ID Data 2 Take a Quiz **CONFIRM WORK ELIGIBILITY** 3 Enter Document Data 4 Get Results

### Possible Mismatch with Social Security Information

Thank you for checking on your work authorization information through Self Check. Unfortunately we were not able to automatically verify the information you provided against Social Security Administration records.

**What does this mean?**

- In order to resolve the mismatch, Social Security Administration staff needs to manually review database records.
- This does not mean that you are not work authorized. It simply means SSA will have to check the data manually before giving you an answer.

**What can you do?**

- 1 SELECT "I WILL VISIT SSA" BUTTON**
- 2 READ & PRINT LETTER**
- 3 VISIT SSA**

1. **SELECT "I WILL VISIT SSA" BUTTON** - If you plan to visit SSA to request further investigation of the issue, please indicate by clicking the "I Will Visit SSA" button below to get additional instructions. Please note that you are not required to follow up about this issue.

2. **READ AND PRINT LETTER** - Read and print the letter which provides a summary of the issue and detailed guidance around your next steps.

3. **VISIT SSA** - If you decide to visit SSA, please be sure to bring the letter with you to assist SSA in investigating the issue.

U.S. Department of Homeland Security : dhs.gov U.S. Citizenship and Immigration Services : uscis.gov Accessibility

**Self Check**

Self Check Home  
About Self Check  
How To Use Self Check  
Know Your Rights  
Our Commitment To Privacy  
Questions And Answers  
For Employers

**ESTABLISH IDENTITY** 1 Enter ID Data 2 Take a Quiz **CONFIRM WORK ELIGIBILITY** 3 Enter Document Data 4 Get Results

### Possible Mismatch with Immigration Information

Thank you for checking on your work authorization information through Self Check. Unfortunately we were not able to automatically verify the information you provided against Department of Homeland Security (DHS) immigration records.

**What does this mean?**

- In order to make a final determination, Self Check staff needs to manually review database records
- This does not mean that you are not work authorized. It simply means we have to check the data manually before giving you an answer.

**What can you do?**

- 1 SELECT "PLEASE REVIEW" BUTTON**
- 2 READ & PRINT LETTER**
- 3 CALL DHS**

1. **SELECT "REVIEW" BUTTON** - If you want DHS to further review your work eligibility, please indicate by clicking the "Please Review" button below. Please note that this is not required, but is necessary for DHS to continue a review at this time.

2. **READ AND PRINT LETTER** - Once you request additional review, read and print the letter which provides a summary of the issue and detailed guidance around your next steps.

3. **CALL DHS** - Once you have read and printed the letter, please follow the instructions in the letter to call DHS to begin the review process.

U.S. Department of Homeland Security : dhs.gov U.S. Citizenship and Immigration Services : uscis.gov Accessibility

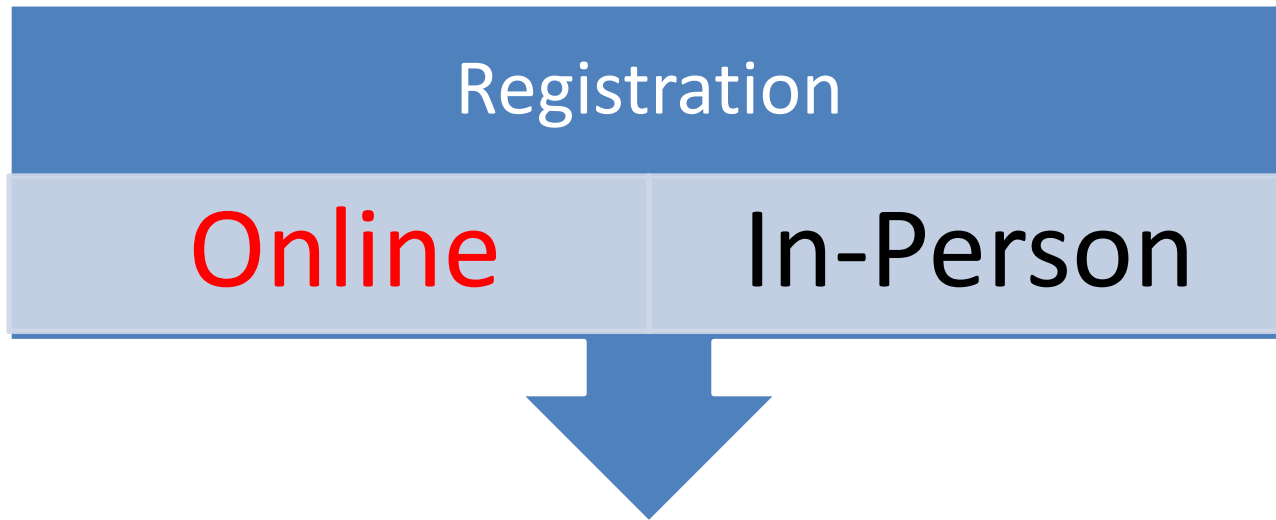


Homeland  
Security

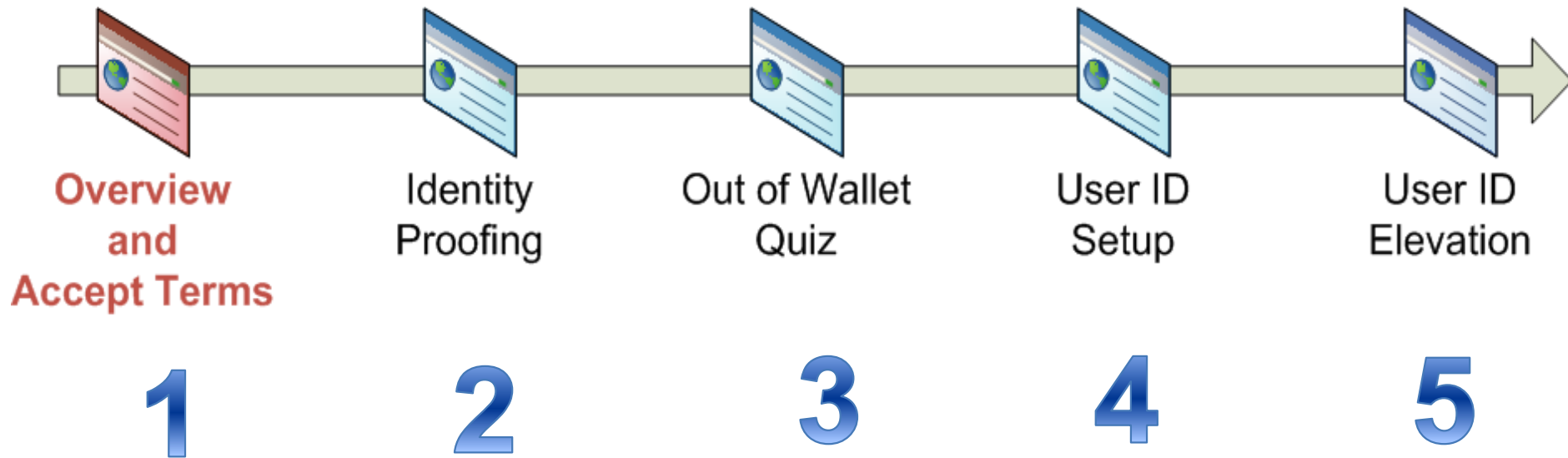
Privacy Office

# ***LOA 2 Example: mySocialSecurity***

## **Focus Today**



# ***The 5 Steps of Registration***





# Sign In or Create an Account

Text Size Accessibility Help



## Social Security

The Official Website of the U.S. Social Security Administration

Sign In or Create an Account

OMB No. 0960-0789  
[Paperwork Reduction Act](#)

### New Users

**You must be able to verify some information about yourself and:**

- have a valid email address,
- have a Social Security Number,
- have a U.S. mailing address, and
- be at least 18 years of age.



[Create An Account](#) [? Learn More](#)

### Existing Users

**Username:**

[▶ Forgot Username](#)

**Password:**

[▶ Forgot Password](#)

[Sign In](#)

Are you now, or have you ever been a victim of domestic violence? Identity theft? Do you have other concerns?

You can [block electronic access](#) to your information at any time, for any reason.



**Homeland  
Security**

Privacy Office

# 1. Overview and Accept Terms

**Social Security**  
The Official Website of the U.S. Social Security Administration

OMB No. 0960-0789  
Paperwork Reduction Act

### Create an Account

#### Terms of Service

You must be able to verify some information about yourself and:

- Have a valid E-mail address,
- Have a Social Security number,
- Have a U.S. mailing address, and
- Be at least 18 years of age.

You can create an account only to gain access to your own personal information. Even with a person's written consent, you cannot use this online service to access the records of a person:

- With whom you have a business relationship; or
- For whom you are an appointed representative.

Unauthorized use of this service may subject you to criminal or civil penalties, or both.

#### What will we do with your information?

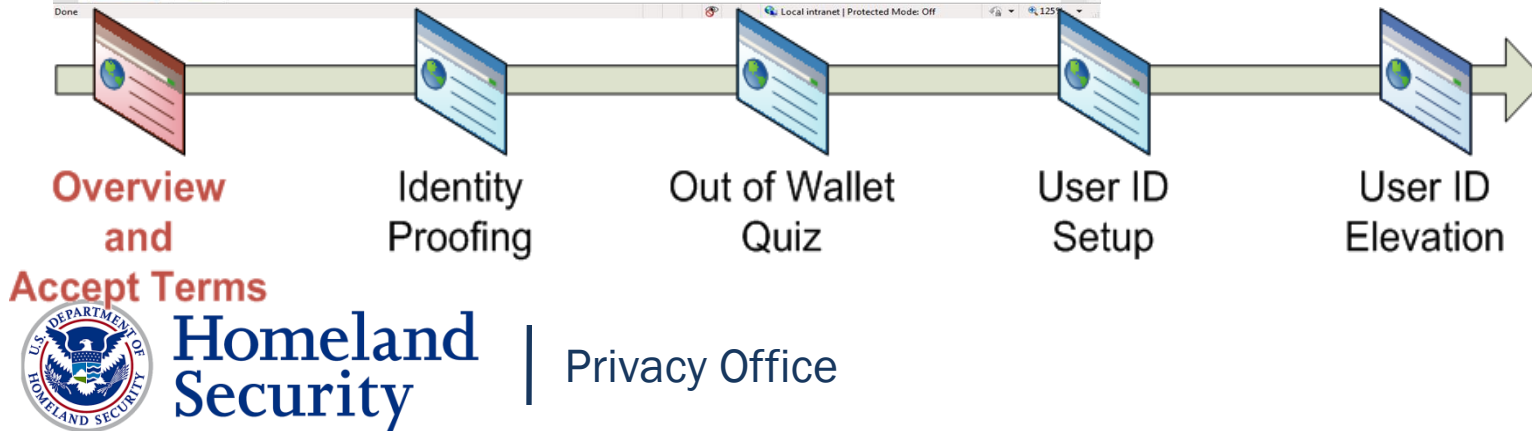
We use the information you give us to verify your identity. We verify the information you give us against our records. We also use Experian, an external authentication service provider, to help us verify your identity. Experian verifies the information you give us against their records. We do not share your Social Security number with Experian. Experian keeps your information only for the time period permitted by Federal laws, Regulations, or guidelines. We use Experian's fraud prevention services to protect you from identity theft.

#### What happens if you provide false information or misuse this service?

You may be subject to criminal or civil penalties, or both, if you provide false or misleading statements to sign in or create an account or engage in unauthorized use of this service.


☒ I agree to the Terms of Service.

**Next** **Exit**



# Identity Proofing

Text Size Accessibility Help

 **Social Security**  
The Official Website of the U.S. Social Security Administration

## Create an Account

1 Verify your Identity 2 Secure your Identity 3 Create your Account

Please tell us who you are

**Your Name:**  
As shown on your Social Security card.

First M.I. Last Suffix

**Social Security Number (SSN):**


**Date of Birth:**

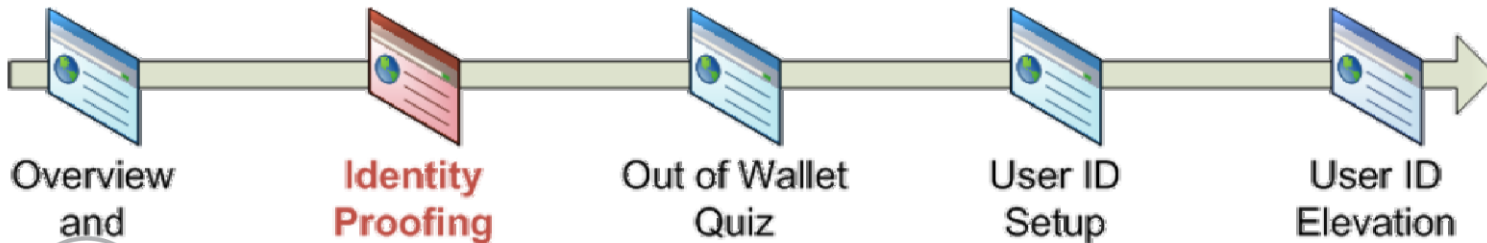
Month Day Year

**Home Address:**  
We cannot accept a business address unless it is also the place where you live. The information you provide here will not update any information we have on file.

Street Line 1: Street Line 2:

City/Town: State/Territory: ZIP Code:

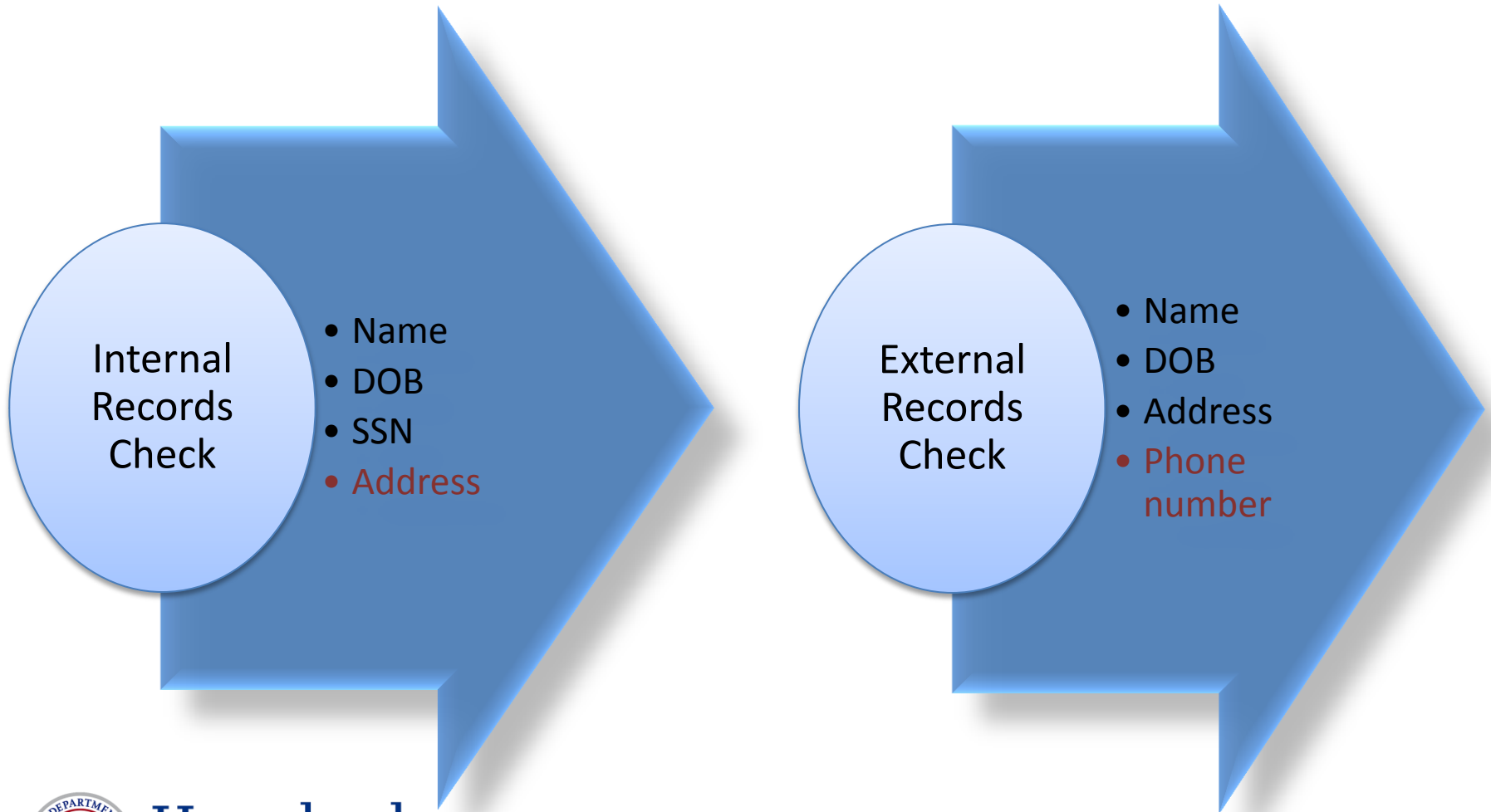
**Privacy & Security**  
Find out more about our policies and procedures.  
  
[Learn More](#)



Homeland Security

Privacy Office

## 2. Identity Proofing



# 3. Out of Wallet Quiz

Text Size Accessibility Help

Social Security  
The Official Website of the U.S. Social Security Administration

## Create an Account

1 Verify your Identity 2 Secure your Identity 3 Create your Account

Please tell us about yourself  
We collect and evaluate this information as a security measure to ensure that only you are able to access your personal information. We will not store your answers.  
[Why are these questions important?](#)

You may have opened an auto loan or auto lease in or around August 2006. Please select the dollar amount range in which your monthly auto loan or lease payment falls. If you have not had an auto loan or lease with any of these amount ranges now or in the past, please select 'NONE OF THE ABOVE/DOES NOT APPLY'.

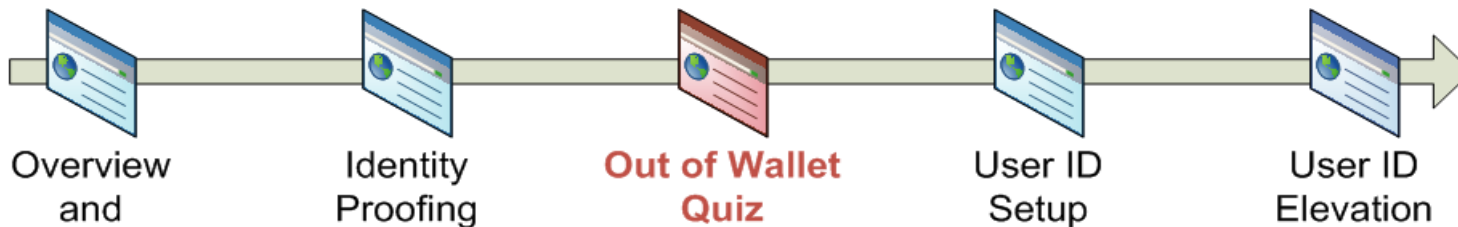
- ☐ \$135 - \$184
- ☐ \$185 - \$234
- ☐ \$235 - \$284
- ☐ \$285 - \$334
- ☐ NONE OF THE ABOVE/DOES NOT APPLY

You may have opened a student loan in or around February 1999. Please select the lender that you have previously or you are currently making payments to. If you have not received student loans with any of these lenders now or in the past, please select 'NONE OF THE ABOVE/DOES NOT APPLY'.

- ☐ KEY CORP
- ☐ GLESLI/STUDENT LOAD FI
- ☐ US DEPT OF EDUCATION
- ☐ USA GROUP LOAN SERVICE
- ☐ NONE OF THE ABOVE/DOES NOT APPLY

**Privacy & Security**  
Find out more about our policies and procedures.  
  
[Learn More](#)

Trusted sites | Protected Mode: Off 125%



Homeland  
Security

Privacy Office

# 4. User ID Setup

Text Size Accessibility Help

**Social Security**  
The Official Website of the U.S. Social Security Administration

Create an Account

1 ✓ Verify your Identity 2 ✓ Secure your Identity 3 Create your Account

Please create your account details

**Username:**  
  
8 to 20 letters and/or numbers  
- cannot be your Social Security Number (SSN)  
- cannot be your name

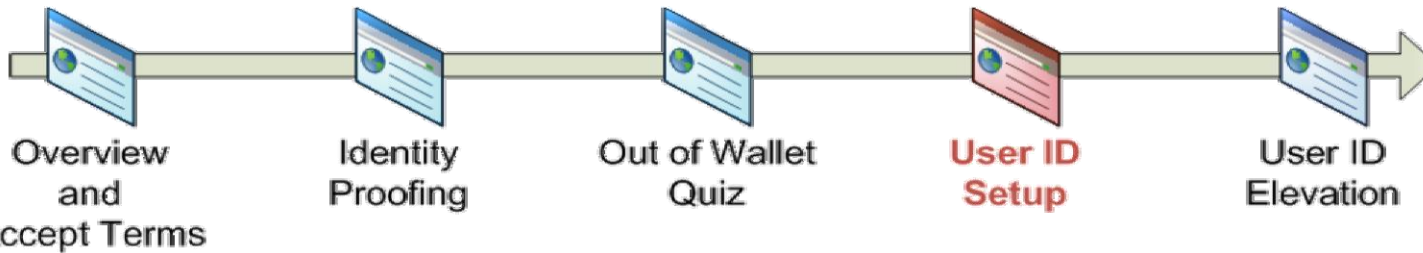
**Password:**  
 Password Strength:   
8 characters minimum and must contain:  
- at least one uppercase letter (A-Z)  
- at least one lowercase letter (a-z)  
- at least one number (0-9)  
- at least one symbol (For example: ! @ # \$ % ^ & \*)

**Confirm Password:**

**Email Address:**  
We need this to communicate with you about your online account.

**Confirm Email Address:**

**Privacy & Security**  
Find out more about our policies and procedures.  
  
[Learn More](#)




**Homeland Security**

Privacy Office

# Current Overview

Drew Jenkins | Sign Out

Text Size ▾ | Accessibility Help

 **my Social Security**

My Home

Help Center

Security Settings


Overview

Estimated Benefits

Earnings Record

**Welcome, Drew!** You last signed in on January 1, 2011 at 3:45 pm EST.

### Social Security Statement



**A Message from the Commissioner:**

- + What Social Security means to you...
- + About Social Security's future...
- + Learn more about Social Security...

Estimated benefit at full retirement (age 67):


\$1,500 a month

[View Estimated Benefits](#)

Last reported earnings:

\$42,492 in 2010

[View Earnings Record](#)

 [Print / Save Your Full Statement](#)  
Get a copy of your Statement information in a convenient, print-friendly format.

+ Drew Jenkins

Email:  
drew\_jenkins@email.com  
[Update Email](#)

Help Center

Find an Office

Privacy Policy



**Homeland  
Security**

Privacy Office




# My Profile

Drew Jenkins

Sign Out

Text Size

Accessibility Help



my Social Security

My Home

Help Center

Security Settings

Overview

Benefit & Payment Details

Earnings Record

My Profile

Personal Information

Your Name: Drew Jenkins

Social Security Number: XXX-XX-1234

Date of Birth: January 1, 1945

Your Address & Phone Number:

Address	Phone Number	For Benefit...
123 Sample Drive Baltimore, MD 12345	(401) 123-4567	Social Security (Retirement), Social Security (Survivors), Medicare

Update Contact Information

Your Email Address: drew.jenkins@email.com

Update Email Address

More Information

How do I correct or update my name or date of birth?

How do I request a new Social Security Card?

How do I update my contact info if I have special needs as a blind or visually impaired user?

Go to Security Settings

Your security settings allows you to update your:

account security options,

password, and

password reset questions.

Direct Deposit Information

With Direct Deposit, your money will go automatically into your account every month. You don't have to wait for a check in the mail or go to your bank to deposit your money. It's safe, quick, and convenient.

Payment / Account Information	For Benefit...
Direct Deposit to: American Bank; Checking; Account Number: x6789 (Last 4 digits)	Social Security (Retirement), Social Security (Survivors)

Update Direct Deposit

Help Center

Find an Office

Privacy Policy



Homeland  
Security

Privacy Office



# ***Recommendations***

- Assess your user population to determine whether knowledge based authentication is feasible.
- Have a plan to address individuals who are unable to electronically authenticate.
- Work with your vendor to monitor quiz generation and quiz pass rates and adjust your quiz strategy as appropriate.
- Work closely with your vendors to fully understand retention and use practices.
- Communicate clearly with your customer base about e-authentication practices.
- Use the PIA, privacy notices, and terms of service process to promote transparency.
- Consider data minimization for data collected for authentication



# Resources

- Self Check
  - <http://www.uscis.gov/self-check>
  - PIA (<http://www.dhs.gov/publication/dhsuscispia-030b-e-verify-self-check>)
  - SORN (<http://edocket.access.gpo.gov/2011/2011-3490.htm>,  
<http://www.gpo.gov/fdsys/pkg/FR-2013-07-22/html/2013-17451.htm>)
- mySocialSecurity
  - <http://ssa.gov/myaccount/>
  - PIA (<http://www.socialsecurity.gov/foia/piadocuments/FY11/e-Auth%20PIA%20May%2031%202011.htm>)
  - SORN (<http://www.socialsecurity.gov/foia/bluebook/60-0373.htm>)



# ***Interactive Exercise***

The United States National Park Service (USNPS) operates an online permit application process. Nancy Naturelover would like visit the Grand Canyon over the July 4<sup>th</sup> weekend and would like to rent a campsite. As this is a highly coveted weekend, there is more demand than campsites available. The USNPS allows members of the public to sign up on line for a campsite lottery that they hold at the beginning of the summer.

To enter the lottery, the USNPS requires interested members of the public to provide their name, address and telephone number to enter the lottery. Wining members of the lottery provide payment when they arrive at the campsite.



# ***Discussion Questions***

- What level of assurance do you think this should be?
- What data elements do you think USNPS should collect to administer the lottery?
- Does your level of assurance decision change if the individual must provide credit card information that is automatically charged upon a successful bid?
- As a privacy professional, what advice would you give USNPS in setting up this lottery?
- What additional questions would you ask USNPS about this service?



# Creating a Culture of Privacy: Privacy Training & Awareness

**Peter Miller**

Federal Trade Commission  
Chief Privacy Officer

**Steve Richards**

Dept. of Homeland Security  
Associate Director  
Communications & Training

# PRIVACY

# WHAT'S THE PRIVACY CHALLENGE?

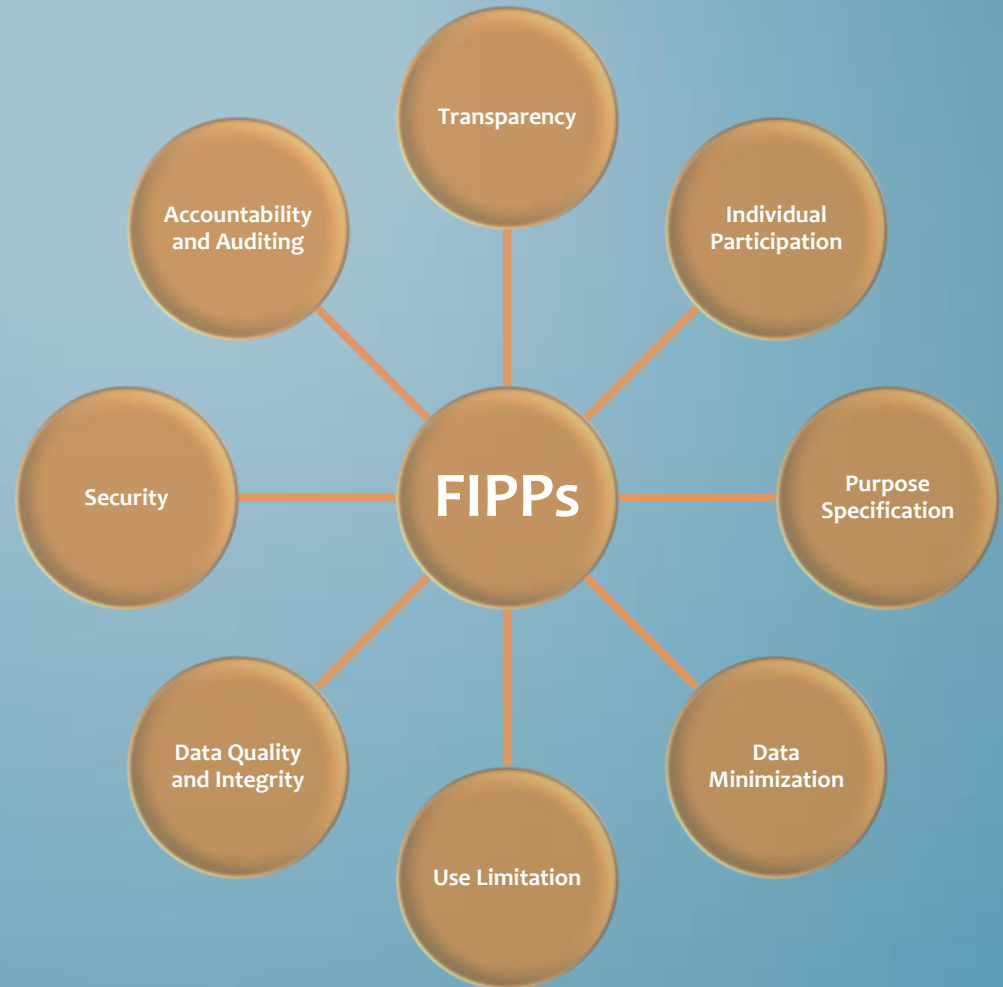
- To increase awareness while vulnerabilities are increasing:
  - *Phishing*
  - *Social media*
  - *Human error*
  - *Larger volume and flow of information*
- Technical controls can't eliminate all of the risks!

## WHAT'S THE SOLUTION?

- *Build a culture of privacy with an effective privacy training and awareness program*

# FAIR INFORMATION PRACTICE PRINCIPLES

- Transparency
  - TR – 1 - 3
- Individual Participation
  - IP – 1 - 4
- Purpose Specification
  - AP – 1 & 2
- Data Minimization
  - DM – 1 - 3
- Use Limitation
  - UL – 1 & 2
- Data Quality and Integrity
  - DI – 1 & 2
- Security
  - SE – 1 & 2
- Accountability and Auditing
  - AR – 1 - 8





# LEARNING OBJECTIVES

- Understand your role in protecting privacy and promoting our privacy culture
- Know how to identify PII
- Protect PII in different contexts and formats
- Recognize and report a privacy incident

# TRAINING AND AWARENESS BEST PRACTICES

## Staff training:

- *New employees*
- *Annual refresher training*
- *Role-based training*
- *Incident response training*

# TRAINING AND AWARENESS BEST PRACTICES

## Awareness campaigns:

- *Email tips, newsletters*
- *Intranet site*
- *Events/workshops*
- *Posters/flyers/factsheets*

USCIS Second Annual Privacy Awareness Week 2012  
Tomich Conference Center/Verification Division  
April 23rd-27th, 2012

**Monday, April 23, 2012 (Tomich Conference Center)**

- 1:00 p.m. to 1:30 p.m. Opening Remarks: Lori Scialabba, Deputy Director, USCIS
- 1:30 p.m. to 1:35p.m. Welcome: Donald K. Hawkins, Chief, USCIS Privacy Office
- 1:35 p.m. to 2:35p.m. Keynote Speaker: Mary Ellen Callahan, Chief, DHS Privacy Office  
**Topic:** Privacy and Social Media
- 2:35 p.m. to 3:00 p.m. Annual Privacy Awareness Training

**Tuesday, April 24, 2012 (Verification Division Large Conference Room)**

- 10:00 a.m. to 11:30 a.m. Annual Privacy Awareness Training
- 1:00 p.m. to 2:00 p.m. Sandy Ford Page, Chief, Business Operations for the Office of Risk Management and Analysis, National Protection and Programs Directorate (NPPD)  
**Topic:** Identity Theft
- 2:00 p.m. to 3:00 p.m. John Mazza, Special Agent, United States Secret Service (USSS)  
**Topic:** USSS Jurisdictional History; The Proliferation of Identity Theft

**Wednesday, April 25, 2012 (Tomich Conference Center)**

- 10:00 a.m. to 11:30 a.m. Annual Privacy Awareness Training
- 1:00 p.m. to 2:30 p.m. "Movie Day" with popcorn (Theme: privacy-issue focused)  
Donald Hawkins, Chief Privacy Officer  
Brian Hobbs, Chief, Verification Privacy Branch

**Thursday, April 26, 2012 (Tomich Conference Center)**

- 10:00 a.m. to 11:30 a.m. Annual Privacy Awareness Training
- 1:00 p.m. to 2:00 p.m. Steven Toporoff, Attorney, Federal Trade Commission (FTC)  
**Topic:** Child Identity Theft
- 2:00 p.m. to 3:00 p.m. Rebekah Meservy, Appraisal Archivist, National Archives & Records Administration (NARA)  
**Topic:** Protecting private information within and from your records

**Friday, April 27, 2012**

- All Day National Clean Up Day – Come Relaxed and Ready to Shred!

# Privacy Awareness



**PRIVACY:**  
**DON'T BE A**  
**TARGET**



U.S. Citizenship  
and Immigration  
Services



# EVERYONE CAN BE A PRIVACY SUPERHERO

Visit the Privacy Homepage  
to learn what you can do  
to protect your privacy and  
other people's.

## PRIVACY WEEK

April 30 - May 4, 2012





# PrivacyMan

Privacy is everywhere!

Build privacy into your program!

See "Things you should know-program manager" on the intranet  
Intranet resources under "Privacy Policy" link

**E-mail us: [TSAprivacy@dhs.gov](mailto:TSAprivacy@dhs.gov)**



Transportation  
Security  
Administration



# MEASURE YOUR IMPACT

- *Employee surveys*
- *Course completions*
- *Incident reporting*
- *Websites*



Don't Have a MAX ID Yet?

[Register Now](#)



Learn about

## MAX Cloud Services

Available for use by **agencies** for **any cross-government** or **intra-agency activity**

[www.MAX.gov](http://www.MAX.gov)

[Learn More](#)

1 2 3

[Login](#)

[Manage Your Password](#)

[MAX Cloud Services Capabilities](#)

[Budget Formulation and Execution Line of Business](#)

### Welcome to the MAX Homepage

If you are a new user, please [register here](#). Registration is **ONLY** available to Federal government employees and contractors with a valid .gov, .mil, or .fed.us email address. Please visit our [FAQ](#) for any questions about accessing MAX or to view our user agreement.

### MAX Federal Community

The MAX Federal Community is used by OMB and Federal agencies to share information and collaborate. It is part of the Budget Formulation and Execution Line of Business (BFELoB).

[Go to MAX Federal Community](#)

### Apportionment

OMB Circular A-11 requires all executive branch agencies to use OMB's web-based apportionment system to send apportionment requests to OMB. Agency budget offices use the apportionment application to: help prepare apportionment requests; send requests to OMB; and, run reports against previously approved apportionments. OMB examining divisions use the application to send electronic copies of approved apportionment to agencies, and, run reports against previously approved apportionments.

[Go to Apportionment](#)

### Hours of Operation

#### Weekdays

Available 24 hours

Support available 8:30 AM-6:30 PM EST

#### Weekends

Available all hours except Sun 2AM-8AM EST

Support available 9AM-6PM EST (response within 2 hours)

### Contact Us

#### E-Mail

[maxsupport@omb.eop.gov](mailto:maxsupport@omb.eop.gov)

#### Phone

202-395-6860







All

Q



 (2)  (0)

 Edit

[+ Add Content](#)

★ Favorites ▾

 Share

✉ Watchers (107)



## About the Privacy Committee

Privacy Committee Activities Include:

- Training Boot Camps
- Privacy Workshops

## TBD

The Privacy Committee shall perform functions that include the following:

- Develop recommendations for OMB on federal government privacy policies and requirements.
- Share experiences, ideas, best practices, and innovative approaches related to protection of privacy and implementation of appropriate safeguards.
- Advise the full CIO Council on privacy related matters and coordinate with other CIO Council committees on topics of mutual concern as needed.



E-GOVERNMENT COMMUNITY

# Federal CIO Council - Privacy Training and Awareness Best Practices

Search The MAX Community

All

OPEN - EXECUTIVE BRANCH

E-GovernHomeE-Gov CoFederal CIO Council Privacy CommitteeFederal CIO Council - Privacy Training and Awareness Best Practices (5)

(2) (0)

Edited By Steven Richards(DHS) on May 03, 2012 at 04:22 PM

EditAdd ContentFavoritesShareWatchers (4)

PAGE TREE

HomePrivacy TrainingPrivacy AwarenessMetricsPrivacy Resources

## Introduction

This site is a resource for all federal privacy offices developing or expanding a privacy training and awareness program in order to build a culture of privacy within an organization. Studies on the causes of data breaches show that most occur due to unintentional error by an organization's staff, rather than malicious acts. Therefore, staff can and should be trained to protect personal information or Personally Identifiable Information (PII).

- [DHS:Top 5 Mistakes of Privacy Awareness Programs \(PDF\)](#)
- [DHS:Data Beach Mistakes Feared More Than Hackers by Compliance Professionals \(PDF\)](#)

To create an effective privacy training and awareness program with limited resources, follow the best practices detailed on this site.

## Feedback

If you have questions or want to submit content to be considered for publication on this site, please email Steve Richards at: [steven.richards@hq.dhs.gov](mailto:steven.richards@hq.dhs.gov)

## Background

A privacy training and awareness program is more effective if your privacy office is founded on a privacy risk management framework [DHS:e.g., the Fair Information Practice Principles], as well as good privacy policies.

Effective privacy stewardship includes:

1. Organizational commitment to privacy
2. Privacy risk mitigation in operations

## ADDITIONAL RESOURCES

- *FTC.gov*
- *Steven.richards@hq.dhs.gov*
- *pmiller@ftc.gov*





Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



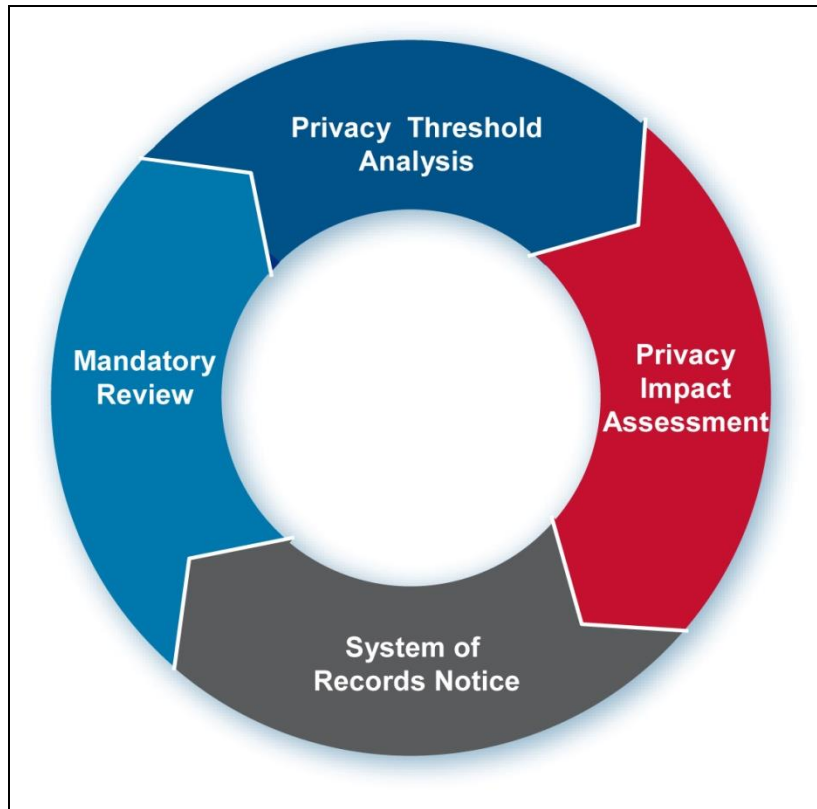
# *Privacy Compliance Reviews*

Debra Danisek, Associate Director

---

Privacy Oversight  
DHS Privacy Office

# *Privacy Compliance Lifecycle*



## **Privacy Compliance Artifacts**

- Privacy Threshold Analysis (PTA)
- Privacy Impact Assessment (PIA)
- System of Records Notice (SORN)
- Privacy Compliance Review (PCR)





# *Privacy Compliance Reviews at DHS*

- **PCR Goals:**
  - PCRs are a *constructive* mechanism to:
    - Assess implementation of protections described in documentation
    - Identify areas for improvement, and
    - Correct course if necessary.
- Relatively new function, created in 2011.
- Part of the Oversight Team, formerly part of the Compliance Team



# *Privacy Compliance Reviews at DHS*

- Unique position of DHS Privacy Office:
  - Both an advisor and an oversight body for the Department's privacy sensitive programs and systems
  - PCR is designed to improve a program's ability to comply with assurances made in privacy compliance documentation (e.g., privacy policy, Privacy Impact Assessment).
- PCRs can be initiated:
  - At the discretion of the DHS Chief Privacy Officer
  - As required by an Agreement
  - Under the terms of a Privacy Impact Assessment





# *PCR Process Steps*

## **Step 1: Collect and Review Available Background Information**

- Background sources:
  - Applicable Privacy Impact Assessment(s) and System of Records Notice(s)
  - Relevant compliance and policy documents such as Memoranda of Understanding (MOUs) and Information Sharing Access Agreements (ISAAs)
  - Publicly available information such as the program website and applicable DHS Inspector General and Government Accountability Office reports.
- The statements in the **PIA** and **SORN** will serve as the **baseline** for assessing a program's compliance.



# *PCR Process Steps*

## **Step 2: Formulate Review Objectives**

- The first objective of any privacy review is to **assess a program's compliance with current privacy documentation, and applicable DHS policies.**
- PRIV may also determine other objectives from:
  - MOUs and Agreements
  - Previous reports (OIG or GAO)
  - Other privacy-related concerns voiced from the public or other medium (e.g., newspaper reports program does X in violation of privacy, and Privacy Office specifically reviews and assesses the claim).



# PCR Process Steps

## Step 3: Notify Program of Review

- *Buy-in from program and leadership is critical!*
- The Oversight Group notifies the Component Privacy Officer/Privacy Point of Contact and Program Manager of PRIV's intent to conduct a review of the program with **clearly stated review objectives**.



# *PCR Process Steps*

## **Step 4: Formulate Review Questions and Document Requests**

- Develop a set of tailored questions to the specific program/IT system.
- To the extent any other documentation needs can be identified up front, these should be included with the tailored questions sent to the program.
  - Documents requested may include standard operating procedures, policies, and system audit logs and will vary depending on the scope of the review.



# *PCR Process Steps*

## **Step 5: Conduct Interviews and Obtain Supporting Documents**

- Two primary mechanisms for compliance reviews:
  - Interviews with program personnel; and
  - Document reviews
- The initial interview should be conducted in person
- If the Oversight Group finds that references are made to a policy, procedure or other written artifact that can substantiate the program's statements, request a copy of the document for analysis.
- Document the results of the meeting.



# *PCR Process Steps*

## **Step 6: Analyze Documentation and Interviews and Document Preliminary Conclusions**

- Review documentation and evaluate against statements made in privacy compliance documentation.
- Document review may also include activities such as review of audit logs to ensure uses of information are appropriate.



# *PCR Process Steps*

## **Step 7: Review and Confirm Findings**

- Notify the program of preliminary findings and recommendations from the record of analysis and confirm key facts contained within.
  - This will often be achieved through sharing a draft product with the reviewed program for their review and comment.
- Determine the appropriate format and content for documenting the results of the PCR including any recommendations that should be communicated to the program.



# *PCR Process Steps*

## **Step 8: Prepare and Issue Product**

- PCRs may result in a public report or an internal memoranda to the program principal signed by the Chief Privacy Officer.
- Provide the program and the affected Component Privacy Officer or Privacy Point of Contact an opportunity to review and comment on a draft product and will make revisions accordingly.





# *What are the potential outcomes and benefits of a PCR?*

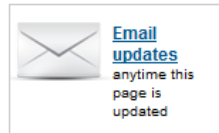
- Recommendations to the program resulting in improvements
- Updates to privacy documentation
- Informal discussions about lessons learned
- Formal report either internal or publicly available
- Heightened awareness by all participants about privacy
- Early issue identification and remediation



# DHS PCRs Online



[Home](#) > [Privacy Investigations & Compliance Reviews](#)



## Privacy Investigations & Compliance Reviews

### Privacy Investigations

In accordance with the Homeland Security Act of 2002, Section 222a (1) (as modified), the Department of Homeland Security (DHS) Chief Privacy Officer is authorized to...make such investigations and reports relating to the administration of the programs and operations of the Department as are, in the senior official's judgment, necessary or desirable.

[OIG Privacy Incident Report and Assessment](#), February 2011, (PDF, 45 pages - 1.01 MB)  
Chief Privacy Officer (CPO) Mary Ellen Callahan issued a public report on a privacy incident involving the Office of Inspector General (OIG) and contractor KPMG. The report makes findings and recommendations addressing compliance with privacy policies and recommends steps for prevention and mitigation of similar privacy incidents.

### Compliance Reviews

The DHS Privacy Office exercises its authority under Section 222 of the Homeland Security Act to assure that technologies sustain and do not erode privacy protections through the conduct of Privacy Compliance Reviews (PCRs). Consistent with the Privacy Office's unique position as both an advisor and oversight body for the Department's privacy sensitive programs and systems, the PCR is designed as a constructive mechanism to improve a program's ability to comply with assurances made in existing privacy compliance documentation including Privacy Impact Assessments (PIAs), System of Records Notices (SORNs) and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreements.

#### Homeland Security Office

- [DHS Privacy Office](#)

<http://www.dhs.gov/privacy-investigations-compliance-reviews>



Homeland  
Security

Privacy Office

Questions? More information about PCRs?

Debra Danisek

(202) 343-1717

[Debra.Danisek@hq.dhs.gov](mailto:Debra.Danisek@hq.dhs.gov)



**Homeland  
Security**

| Privacy Office



Homeland  
Security

Privacy Office

Protecting privacy while promoting transparency



# *Privacy Incident Response Best Practices*

Kate Claffie

---

Associate Director,  
Privacy Oversight

# ***Topics***

- Why is Privacy Important?
- What is Personally Identifiable Information (PII)?
- What is Sensitive PII?
- Office of Management and Budget Guidance
- Privacy Incident Reporting at DHS
- Best Practices



# ***Why is Privacy Important?***

- To earn and keep public and employee trust
  - If the public or your employees no longer trust your agency to protect their PII, public and employee support may erode.
- To prevent privacy incidents
  - Incidents reported in national news erodes public and employee trust in your agency, and are expensive to mitigate.
- To prevent identity theft
  - Privacy incidents that raise the risk of identity theft can be lengthy, costly, and stressful to recover from for the individual and your agency.
- It's the law
  - Failure to follow these laws may result in civil or criminal penalties, or loss of employment.



# ***Personally Identifiable Information (PII)***

- Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to an individual.
- DHS uses a broad definition of PII and extends privacy protections regardless of whether the individual is a U.S. Citizen, Legal Permanent Resident, or a visitor to the U.S.



# ***Personally Identifiable Information (PII)***

- PII includes:
  - Name
  - Date of Birth
  - Mailing address, phone number, and/or email address
  - Social Security number (SSN)
  - Other Government-issued numbers (e.g., Passport, Alien Registration, driver's license)
  - Account numbers
  - Biometric identifiers





# ***Sensitive PII***

- Potential for substantial harm, embarrassment, inconvenience, or unfairness to an individual if compromised
- Single data elements
  - Social Security number, driver's license or state identification number, Passport number, Alien Registration Number, or financial account number
- Combinations of data
  - citizenship or immigration status; medical information; ethnic, religious, sexual orientation; account passwords
- Context of data
  - a list of employees with poor performance ratings.



# Office of Management and Budget Guidance:

*The Foundation for Incident Reporting*



**Homeland  
Security**

| Privacy Office

# ***Office of Management and Budget Guidance***

- OMB Memorandum 06-15, ***Safeguarding Personally Identifiable Information*** (May 22, 2006)
  - Emphasizes agency responsibilities to safeguard Sensitive PII and train employees on their responsibilities for protecting privacy.
- OMB Memorandum 06-19, ***Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*** (July 23, 2006)
  - Requires agencies to report all incidents (actual or potential) involving PII to US-CERT within one hour of discovery of the incident.



# ***Office of Management and Budget Guidance***

- OMB Memorandum, ***Recommendations for Identity Theft Related Data Breach Notification*** (September 20, 2006)
  - Provides recommendations from the President's Identity Theft Task Force to develop planning and response procedures addressing PII incidents that could result in identify theft.
- OMB Memorandum 07-16, ***Safeguarding Against and Responding to the Breach of Personally Identifiable Information*** (May 22, 2007)
  - Each agency must develop an incident response plan.
  - Sets requirements for remote access and portable devices.
  - Requires development of policies and procedures for reporting and mitigating PII incidents, and for notification of privacy incidents (actual or potential) to US-CERT within one hour of discovery.



# Privacy Incident Reporting at DHS



**Homeland  
Security**

| Privacy Office

# ***What is a Privacy Incident?***

- The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any other situation where persons other than authorized users have access or potential access to PII in usable form, or where authorized users access PII for an unauthorized purpose.
- Involves PII in physical (hard copy) or electronic form.
- Includes suspected or confirmed privacy incidents.



# ***Types of Harms Resulting from a Privacy Incident***

- Harm to an Agency:
  - Undermining the integrity or security of a system or program
  - Embarrassment
  - Reputation
- Harm to an individual:
  - Identity theft
  - Embarrassment
  - Harassment
  - Unfairness



# ***Examples of Privacy Incidents***

- E-mail containing payroll information sent from a government e-mail account to a personal e-mail account.
- Theft of an unencrypted laptop containing benefit application information.
- Lost or stolen thumb drive or portable hard drive containing PII.
- E-mail containing Sensitive PII sent internally to an individual who had no need to know.
- A package of employee applications lost in the mail.
- Unauthorized access to personnel files.
- Documents containing PII thrown in a garbage can.





# ***DHS Privacy Incident Handling Guidance (PIHG)***

- Developed in conjunction with:
  - DHS Chief Information Officer (CIO) and Chief Information Security Officer (CISO)
- Provides privacy incident identification and handling guidance
- Includes checklists for all stages of privacy incident handling
- Addresses all types of privacy incidents (paper, electronic, web-based, or physical occurrence)



# ***DHS Privacy Incident Handling Guidance (PIHG)***

- Originally issued in September 2007
- Revised and reissued on January 26, 2012 to streamline processes and incorporate lessons learned since 2007
- DHS Security Operations Center (SOC) Standard Operating Procedures also include Privacy Incident reporting procedures



# ***Reporting a Privacy Incident at DHS***

- Individual notifies Program Manager (PM) of potential or actual loss or disclosure of PII
  - Or –
- PM and/or Component Privacy Officer/Privacy Point of Contact (PPOC) notifies component Information System Security Manager (ISSM) of potential or actual loss or disclosure of PII
- ISSM and/or PPOC completes initial Privacy Incident Report Template in the DHS SOC Online Reporting System



# ***Reporting a Privacy Incident at DHS***

- DHS SOC Online notifies US-CERT and sends an automatic email alert message with initial Privacy Incident report to:
  - Component ISSM and Component Privacy Officer/PPOC
  - DHS Privacy Office Oversight Team
  - DHS Office of Inspector General
- If the privacy incident is significant, DHS SOC also notifies:
  - DHS Chief Privacy Officer
  - DHS Chief Information Officer (CIO) and Deputy CIO
  - DHS Chief Information Security Officer (CISO) and Deputy CISO
  - Component Head



# ***Privacy Incident Handling – Steps***

- Component Privacy Officer or PPOC/ISSM performs the following steps for every privacy incident:
  - **Escalation** – identify who in the component’s management team should be notified, and whether outside entities need to be involved (e.g., local law enforcement, financial entities)
  - **Investigation** – conducted by the Component Privacy Officer or PPOC/ISSM, as well as by the OIG or law enforcement as warranted
  - **Notification** – evaluate need for notification of affected individuals of the actual or potential loss/compromise of PII
  - **Remediation** – determine corrective and protective actions to be taken to minimize loss and/or harm to individuals and Component/Department
  - **Closure** – recommend closure upon completion of mitigation/remediation of privacy incident



# ***Risk Assessment: Five Factors***

- During the privacy incident handling process, these five factors are continuously reviewed as information is discovered:
  - Nature of data elements involved.
  - Number of individuals affected.
  - Likelihood that PII is accessible and usable.
  - Likelihood that the privacy incident may lead to harm.
  - Ability of Component to mitigate the risk of harm.



# ***Final Closure of a Privacy Incident***

- DHS Privacy Office reviews all requests for closure of privacy incidents
  - The DHS Privacy Office is the final decision maker
  - The DHS Privacy Office updates the privacy incident report on DHS SOC Online to close an incident
  - DHS Privacy Office provides oversight for all privacy incidents and maintains statistical and historical data on incident reporting



# Best Practices

*Lessons-learned over the past 7 years*



**Homeland  
Security**

| Privacy Office



# ***Best Practices***

- Constant communication between DHS Privacy Office, Component Privacy Officers/PPOCs, and DHS SOC
- Regular Privacy Incident Handling Meetings
  - Provide statistics and highlight trends
  - Presentations on relevant topics (e.g., hacking, training)
- Using anonymized examples for training
- Leveraging expertise of DHS SOC for technical-related privacy incidents and emerging IT-related issues
- Collaborating with staff on privacy training, tip sheets, and guidance related to privacy incidents
  - Incorporating privacy incident scenarios into mandatory privacy training
  - Providing customizable tip sheets on requested or high profile topics



**Kathleen Claffie**

**Associate Director, Privacy Oversight**

DHS Privacy Office

[Kathleen.Claffie@hq.dhs.gov](mailto:Kathleen.Claffie@hq.dhs.gov)

202-343-1744



**Homeland  
Security**

| Privacy Office



# Homeland Security